

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

Absender: INTERNATIONALE RECHERCHENBEHÖRDE

PCT

An

SCHOPPE, ZIMMERMANN & STÖCKELER
z.H. Schoppe, Fritz
Postfach 71 08 67
81458 München
GERMANY

EINGEGANGEN

27. JULI 2000

MITTEILUNG ÜBER DIE ÜBERMITTLUNG DES
INTERNATIONALEN RECHERCHENBERICHTS
ODER DER ERKLÄRUNG

(Regel 44.1 PCT)

Absendedatum
(Tag/Monat/Jahr)

25/07/2000

Aktenzeichen des Anmelders oder Anwalts

FH991202.PCT

WEITERES VORGEHEN

siehe Punkte 1 und 4 unten

Internationales Aktenzeichen

PCT/EP 99/ 09981

Internationales Anmeldedatum

(Tag/Monat/Jahr)

15/12/1999

Anmelder

FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWAND

1. ☒ Dem Anmelder wird mitgeteilt, daß der internationale Recherchenbericht erstellt wurde und ihm hiermit übermittelt wird.

Einreichung von Änderungen und einer Erklärung nach Artikel 19:

Der Anmelder kann auf eigenen Wunsch die Ansprüche der internationalen Anmeldung ändern (siehe Regel 46):

Bis wann sind Änderungen einzureichen?

Die Frist zur Einreichung solcher Änderungen beträgt üblicherweise zwei Monate ab der Übermittlung des internationalen Recherchenberichts; weitere Einzelheiten sind den Anmerkungen auf dem Beiblatt zu entnehmen.

Wo sind Änderungen einzureichen?

Unmittelbar beim Internationalen Büro der WIPO, 34, CHEMIN des Colombettes, CH-1211 Genf 20,
Telefaxnr.: (41-22) 740.14.35

Nähere Hinweise sind den Anmerkungen auf dem Beiblatt zu entnehmen.

2. ☐ Dem Anmelder wird mitgeteilt, daß kein internationaler Recherchenbericht erstellt wird und daß ihm hiermit die Erklärung nach Artikel 17(2a) übermittelt wird.

3. ☐ Hinsichtlich des Widerspruchs gegen die Entrichtung einer zusätzlichen Gebühr (zusätzlicher Gebühren) nach Regel 40.2 wird dem Anmelder mitgeteilt, daß

☐ der Widerspruch und die Entscheidung hierüber zusammen mit seinem Antrag auf Übermittlung des Wortlauts sowohl des Widerspruchs als auch der Entscheidung hierüber an die Bestimmungsämter dem Internationalen Büro übermittelt worden sind.

☐ noch keine Entscheidung über den Widerspruch vorliegt; der Anmelder wird benachrichtigt, sobald eine Entscheidung getroffen wurde.

4. **Weiteres Vorgehen:** Der Anmelder wird auf folgendes aufmerksam gemacht:

Kurz nach Ablauf von **18 Monaten** seit dem Prioritätsdatum wird die internationale Anmeldung vom Internationalen Büro veröffentlicht. Will der Anmelder die Veröffentlichung verhindern oder auf einen späteren Zeitpunkt verschieben, so muß gemäß Regel 90 bis bzw. 90bis vor Abschluß der technischen Vorbereitungen für die internationale Veröffentlichung eine Erklärung über die Zurücknahme der internationalen Anmeldung oder des Prioritätsanspruchs beim Internationalen Büro eingehen.

Innerhalb von **19 Monaten** seit dem Prioritätsdatum ist ein Antrag auf internationale vorläufige Prüfung einzureichen, wenn der Anmelder den Eintritt in die nationale Phase bis zu 30 Monaten seit dem Prioritätsdatum (in manchen Ämtern sogar noch länger) verschieben möchte.

Innerhalb von **20 Monaten** seit dem Prioritätsdatum muß der Anmelder die für den Eintritt in die nationale Phase vorgeschriebenen Handlungen vor allen Bestimmungsämtern vornehmen, die nicht innerhalb von 19 Monaten seit dem Prioritätsdatum in der Anmeldung oder einer nachträglichen Auswahlerklärung ausgewählt wurden oder nicht ausgewählt werden konnten, da für sie Kapitel II des Vertrages nicht verbindlich ist.

Name und Postanschrift der Internationalen Recherchenbehörde



Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL-2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Carole Emery

ANMERKUNGEN ZU FORMBLATT PCT/ISA/220

Diese Anmerkungen sollen grundlegende Hinweise zur Einreichung von Änderungen gemäß Artikel 19 geben. Diesen Anmerkungen liegen die Erfordernisse des Vertrags über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens (PCT), der Ausführungsordnung und der Verwaltungsrichtlinien zu diesem Vertrag zugrunde. Bei Abweichungen zwischen diesen Anmerkungen und obengenannten Texten sind letztere maßgebend. Nähere Einzelheiten sind dem PCT-Leitfaden für Anmelder, einer Veröffentlichung der WIPO, zu entnehmen.

Die in diesen Anmerkungen verwendeten Begriffe "Artikel", "Regel" und "Abschnitt" beziehen sich jeweils auf die Bestimmungen des PCT-Vertrags, der PCT-Ausführungsordnung bzw. der PCT-Verwaltungsrichtlinien.

HINWEISE ZU ÄNDERUNGEN GEMÄSS ARTIKEL 19

Nach Erhalt des internationalen Recherchenberichts hat der Anmelder die Möglichkeit, einmal die Ansprüche der internationalen Anmeldung zu ändern. Es ist jedoch zu betonen, daß, da alle Teile der internationalen Anmeldung (Ansprüche, Beschreibung und Zeichnungen) während des internationalen vorläufigen Prüfungsverfahrens geändert werden können, normalerweise keine Notwendigkeit besteht, Änderungen der Ansprüche nach Artikel 19 einzureichen, außer wenn der Anmelder z.B. zum Zwecke eines vorläufigen Schutzes die Veröffentlichung dieser Ansprüche wünscht oder ein anderer Grund für eine Änderung der Ansprüche vor ihrer internationalen Veröffentlichung vorliegt. Weiterhin ist zu beachten, daß ein vorläufiger Schutz nur in einigen Staaten erhältlich ist.

Welche Teile der internationalen Anmeldung können geändert werden?

Im Rahmen von Artikel 19 können nur die Ansprüche geändert werden.

In der internationalen Phase können die Ansprüche auch nach Artikel 34 vor der mit der internationalen vorläufigen Prüfung beauftragten Behörde geändert (oder nochmals geändert) werden. Die Beschreibung und die Zeichnungen können nur nach Artikel 34 vor der mit der internationalen vorläufigen Prüfung beauftragten Behörde geändert werden.

Beim Eintritt in die nationale Phase können alle Teile der internationalen Anmeldung nach Artikel 28 oder gegebenenfalls Artikel 41 geändert werden.

Bis wann sind Änderungen einzureichen?

Innerhalb von zwei Monaten ab der Übermittlung des internationalen Recherchenberichts oder innerhalb von sechzehn Monaten ab dem Prioritätsdatum, je nachdem, welche Frist später abläuft. Die Änderungen gelten jedoch als rechtzeitig eingereicht, wenn sie dem Internationalen Büro nach Ablauf der maßgebenden Frist, aber noch vor Abschluß der technischen Vorbereitungen für die internationale Veröffentlichung (Regel 46.1) zugehen.

Wo sind die Änderungen nicht einzureichen?

Die Änderungen können nur beim Internationalen Büro, nicht aber beim Anmeldeamt oder der Internationalen Recherchenbehörde eingereicht werden (Regel 46.2).

Falls ein Antrag auf internationale vorläufige Prüfung eingereicht wurde/wird, siehe unten.

In welcher Form können Änderungen erfolgen?

Eine Änderung kann erfolgen durch Streichung eines oder mehrerer ganzer Ansprüche, durch Hinzufügung eines oder mehrerer neuer Ansprüche oder durch Änderung des Wortlauts eines oder mehrerer Ansprüche in der eingereichten Fassung.

Für jedes Anspruchsblatt, das sich aufgrund einer oder mehrerer Änderungen von dem ursprünglich eingereichten Blatt unterscheidet, ist ein Ersatzblatt einzureichen.

Alle Ansprüche, die auf einem Ersatzblatt erscheinen, sind mit arabischen Ziffern zu numerieren. Wird ein Anspruch gestrichen, so brauchen, die anderen Ansprüche nicht neu numeriert zu werden. Im Fall einer Neunummerierung sind die Ansprüche fortlaufend zu numerieren (Verwaltungsrichtlinien, Abschnitt 205 b)).

Die Änderungen sind in der Sprache abzufassen, in der die internationale Anmeldung veröffentlicht wird.

Welche Unterlagen sind den Änderungen beizufügen?

Begleitschreiben (Abschnitt 205 b)):

Die Änderungen sind mit einem Begleitschreiben einzureichen.

Das Begleitschreiben wird nicht zusammen mit der internationalen Anmeldung und den geänderten Ansprüchen veröffentlicht. Es ist nicht zu verwechseln mit der "Erklärung nach Artikel 19(1)" (siehe unten, "Erklärung nach Artikel 19 (1)").

Das Begleitschreiben ist nach Wahl des Anmelders in englischer oder französischer Sprache abzufassen. Bei englischsprachigen internationalen Anmeldungen ist das Begleitschreiben aber ebenfalls in englischer, bei französischsprachigen internationalen Anmeldungen in französischer Sprache abzufassen.

ANMERKUNGEN ZU FORMBLATT PCT/ISA/220 (Fortsetzung)

Im Begleitschreiben sind die Unterschiede zwischen den Ansprüchen in der eingereichten Fassung und den geänderten Ansprüchen anzugeben. So ist insbesondere zu jedem Anspruch in der internationalen Anmeldung anzugeben (gleichlautende Angaben zu verschiedenen Ansprüchen können zusammengefaßt werden), ob

- i) der Anspruch unverändert ist;
- ii) der Anspruch gestrichen worden ist;
- iii) der Anspruch neu ist;
- iv) der Anspruch einen oder mehrere Ansprüche in der eingereichten Fassung ersetzt;
- v) der Anspruch auf die Teilung eines Anspruchs in der eingereichten Fassung zurückzuführen ist.

Im folgenden sind Beispiele angegeben, wie Änderungen im Begleitschreiben zu erläutern sind:

1. [Wenn anstelle von ursprünglich 48 Ansprüchen nach der Änderung einiger Ansprüche 51 Ansprüche existieren]:
"Die Ansprüche 1 bis 29, 31, 32, 34, 35, 37 bis 48 werden durch geänderte Ansprüche gleicher Numerierung ersetzt; Ansprüche 30, 33 und 36 unverändert; neue Ansprüche 49 bis 51 hinzugefügt."
2. [Wenn anstelle von ursprünglich 15 Ansprüchen nach der Änderung aller Ansprüche 11 Ansprüche existieren]:
"Geänderte Ansprüche 1 bis 11 treten an die Stelle der Ansprüche 1 bis 15."
3. [Wenn ursprünglich 14 Ansprüche existierten und die Änderungen darin bestehen, daß einige Ansprüche gestrichen werden und neue Ansprüche hinzugefügt werden]:
Ansprüche 1 bis 6 und 14 unverändert; Ansprüche 7 bis 13 gestrichen; neue Ansprüche 15, 16 und 17 hinzugefügt. "Oder" Ansprüche 7 bis 13 gestrichen; neue Ansprüche 15, 16 und 17 hinzugefügt; alle übrigen Ansprüche unverändert."
4. [Wenn verschiedene Arten von Änderungen durchgeführt werden]:
"Ansprüche 1-10 unverändert; Ansprüche 11 bis 13, 18 und 19 gestrichen; Ansprüche 14, 15 und 16 durch geänderten Anspruch 14 ersetzt; Anspruch 17 in geänderte Ansprüche 15, 16 und 17 unterteilt; neue Ansprüche 20 und 21 hinzugefügt."

"Erklärung nach Artikel 19(1)" (Regel 46.4)

Den Änderungen kann eine Erklärung beigelegt werden, mit der die Änderungen erläutert und ihre Auswirkungen auf die Beschreibung und die Zeichnungen dargelegt werden (die nicht nach Artikel 19 (1) geändert werden können).

Die Erklärung wird zusammen mit der internationalen Anmeldung und den geänderten Ansprüchen veröffentlicht.

Sie ist in der Sprache abzufassen, in der die internationale Anmeldung veröffentlicht wird.

Sie muß kurz gehalten sein und darf, wenn in englischer Sprache abgefaßt oder ins Englische übersetzt, nicht mehr als 500 Wörter umfassen.

Die Erklärung ist nicht zu verwechseln mit dem Begleitschreiben, das auf die Unterschiede zwischen den Ansprüchen in der eingereichten Fassung und den geänderten Ansprüchen hinweist, und ersetzt letzteres nicht. Sie ist auf einem gesonderten Blatt einzureichen und in der Überschrift als solche zu kennzeichnen, vorzugsweise mit den Worten "Erklärung nach Artikel 19 (1)".

Die Erklärung darf keine herabsetzenden Äußerungen über den internationalen Recherchenbericht oder die Bedeutung von in dem Bericht angeführten Veröffentlichungen enthalten. Sie darf auf im internationalen Recherchenbericht angeführte Veröffentlichungen, die sich auf einen bestimmten Anspruch beziehen, nur im Zusammenhang mit einer Änderung dieses Anspruchs Bezug nehmen.

Auswirkungen eines bereits gestellten Antrags auf internationale vorläufige Prüfung

Ist zum Zeitpunkt der Einreichung von Änderungen nach Artikel 19 bereits ein Antrag auf internationale vorläufige Prüfung gestellt worden, so sollte der Anmelder in seinem Interesse gleichzeitig mit der Einreichung der Änderungen beim Internationalen Büro auch eine Kopie der Änderungen bei der mit der internationalen vorläufigen Prüfung beauftragten Behörde einreichen (siehe Regel 62.2 a), erster Satz).

Auswirkungen von Änderungen hinsichtlich der Übersetzung der internationalen Anmeldung beim Eintritt in die nationale Phase

Der Anmelder wird darauf hingewiesen, daß bei Eintritt in die nationale Phase möglicherweise anstatt oder zusätzlich zu der Übersetzung der Ansprüche in der eingereichten Fassung eine Übersetzung der nach Artikel 19 geänderten Ansprüche an die bestimmten/ausgewählten Ämter zu übermitteln ist.

Nähere Einzelheiten über die Erfordernisse jedes bestimmten/ausgewählten Amtes sind Band II des PCT-Leitfadens für Anmelder zu entnehmen.

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts FH991202.PCT	WEITERES VORGEHEN siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5	
Internationales Aktenzeichen PCT/EP 99/ 09981	Internationales Anmeldedatum (Tag/Monat/Jahr) 15/12/1999	(Frühestes) Prioritätsdatum (Tag/Monat/Jahr) 16/02/1999
Anmelder FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWAND		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 2 Blätter.

☒ Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. Grundlage des Berichts

- a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.
- ☐ Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.
- b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das
- ☐ in der internationalen Anmeldung in Schriftlicher Form enthalten ist.
- ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.
- ☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.
- ☐ Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. ☐ Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen (siehe Feld I).

3. ☐ Mangelnde Einheitlichkeit der Erfindung (siehe Feld II).

4. Hinsichtlich der Bezeichnung der Erfindung

- ☒ wird der vom Anmelder eingereichte Wortlaut genehmigt.
- ☐ wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der Zusammenfassung

- ☒ wird der vom Anmelder eingereichte Wortlaut genehmigt.
- ☐ wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 4

- ☒ wie vom Anmelder vorgeschlagen
- ☐ weil der Anmelder selbst keine Abbildung vorgeschlagen hat.
- ☐ weil diese Abbildung die Erfindung besser kennzeichnet.
- ☐ keine der Abb.

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04L9/00 H04N7/167

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 7 H04L H04N

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal, WPI Data, INSPEC

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
P, X	US 5 974 144 A (BRANDMAN NAHUM) 26. Oktober 1999 (1999-10-26) Zusammenfassung Spalte 2, Zeile 25 - Zeile 67 Spalte 4, Zeile 1 - Zeile 22 Anspruch 1 Abbildung 1	1, 17, 28, 29
A	EP 0 438 154 A (CANON KK) 24. Juli 1991 (1991-07-24) Zusammenfassung Spalte 3, Zeile 7 - Zeile 50 Spalte 8, Zeile 1 - Zeile 42 Abbildungen 1A, 1B, 2	1-8, 14-19, 21-25, 28, 29



Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen



Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderscher Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderscher Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

18. Juli 2000

Absendedatum des internationalen Recherchenberichts

25/07/2000

Name und Postanschrift der Internationalen Recherchenbehörde
Europäisches Patentamt, P.B. 5818 Patentaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Gautier, L

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

P 99/09981

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 5974144	A	26-10-1999	AU	2542899 A	15-09-1999
			WO	9944364 A	02-09-1999
EP 0438154	A	24-07-1991	JP	3214834 A	20-09-1991
			DE	69126801 D	21-08-1997
			DE	69126801 T	05-02-1998
			US	5159633 A	27-10-1992

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

Absender: MIT DER INTERNATIONALEN VORLÄUFIGEN
PRÜFUNG BEAUFTRAGTE BEHÖRDE

An:

SCHOPPE, Fritz
SCHOPPE, ZIMMERMANN & STÖCKELER
Postfach 71 08 67
81458 München
ALLEMAGNE

PCT

MITTEILUNG ÜBER DIE ÜBERSENDUNG
DES INTERNATIONALEN VORLÄUFIGEN
PRÜFUNGSBERICHTS
(Regel 71.1 PCT)

Absendedatum
(Tag/Monat/Jahr) 30.01.2001

Aktenzeichen des Anmelders oder Anwalts
FH991202PCT

WICHTIGE MITTEILUNG

Internationales Aktenzeichen
PCT/EP99/09981

Internationales Anmeldedatum (Tag/Monat/Jahr)
15/12/1999

Prioritätsdatum (Tag/Monat/Jahr)
16/02/1999

Anmelder
FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG ... et al.

1. Dem Anmelder wird mitgeteilt, daß ihm die mit der internationalen vorläufigen Prüfung beauftragte Behörde hiermit den zu der internationalen Anmeldung erstellten internationalen vorläufigen Prüfungsbericht, gegebenenfalls mit den dazugehörigen Anlagen, übermittelt.
2. Eine Kopie des Berichts wird - gegebenenfalls mit den dazugehörigen Anlagen - dem Internationalen Büro zur Weiterleitung an alle ausgewählten Ämter übermittelt.
3. Auf Wunsch eines ausgewählten Amtes wird das Internationale Büro eine Übersetzung des Berichts (jedoch nicht der Anlagen) ins Englische anfertigen und diesem Amt übermitteln.


4. ERINNERUNG

Zum Eintritt in die nationale Phase hat der Anmelder vor jedem ausgewählten Amt innerhalb von 30 Monaten ab dem Prioritätsdatum (oder in manchen Ämtern noch später) bestimmte Handlungen (Einreichung von Übersetzungen und Entrichtung nationaler Gebühren) vorzunehmen (Artikel 39 (1)) (siehe auch die durch das Internationale Büro im Formblatt PCT/IB/301 übermittelte Information).

Ist einem ausgewählten Amt eine Übersetzung der internationalen Anmeldung zu übermitteln, so muß diese Übersetzung auch Übersetzungen aller Anlagen zum internationalen vorläufigen Prüfungsbericht enthalten. Es ist Aufgabe des Anmelders, solche Übersetzungen anzufertigen und den betroffenen ausgewählten Ämtern direkt zuzuleiten.

Weitere Einzelheiten zu den maßgebenden Fristen und Erfordernissen der ausgewählten Ämter sind Band II des PCT-Leitfadens für Anmelder zu entnehmen.

Name und Postanschrift der mit der internationalen Prüfung beauftragten Behörde

 Europäisches Patentamt
D-80298 München
Tel. +49 89 2399 - 0 Tx: 523656 epmu d
Fax: +49 89 2399 - 4465

Bevollmächtigter Bediensteter

Ahrens, R

Tel. +49 89 2399-8136

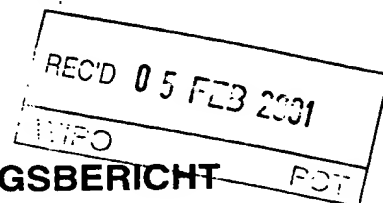


VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)



Aktenzeichen des Anmelders oder Anwalts FH991202PCT	WEITERES VORGEHEN siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsberichts (Formblatt PCT/IPEA/416)	
Internationales Aktenzeichen PCT/EP99/09981	Internationales Anmeldedatum (Tag/Monat/Jahr) 15/12/1999	Prioritätsdatum (Tag/Monat/Tag) 16/02/1999
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK H04L9/00		
Anmelder FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG ... et al.		



- Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationalen vorläufigen Prüfung beauftragten Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.
- Dieser BERICHT umfaßt insgesamt 5 Blätter einschließlich dieses Deckblatts.

☐ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

Diese Anlagen umfassen insgesamt Blätter.

- Dieser Bericht enthält Angaben zu folgenden Punkten:

- I ☒ Grundlage des Berichts
- II ☐ Priorität
- III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
- IV ☐ Mangelnde Einheitlichkeit der Erfindung
- V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
- VI ☐ Bestimmte angeführte Unterlagen
- VII ☐ Bestimmte Mängel der internationalen Anmeldung
- VIII ☐ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags 13/09/2000	Datum der Fertigstellung dieses Berichts 30.01.2001
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde:  Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Bevollmächtigter Bediensteter Bertini, S Tel. Nr. +49 89 2399 8985 

I. Grundlage des Berichts

1. Dieser Bericht wurde erstellt auf der Grundlage (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigelegt, weil sie keine Änderungen enthalten.*):

Beschreibung, Seiten:

1-20 ursprüngliche Fassung

Patentansprüche, Nr.:

1-30 ursprüngliche Fassung

Zeichnungen, Blätter:

1/4-4/4 ursprüngliche Fassung

2. Hinsichtlich der **Sprache**: Alle vorstehend genannten Bestandteile standen der Behörde in der Sprache, in der die internationale Anmeldung eingereicht worden ist, zur Verfügung oder wurden in dieser eingereicht, sofern unter diesem Punkt nichts anderes angegeben ist.

Die Bestandteile standen der Behörde in der Sprache: zur Verfügung bzw. wurden in dieser Sprache eingereicht; dabei handelt es sich um

- ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen Recherche eingereicht worden ist (nach Regel 23.1(b)).
- ☐ die Veröffentlichungssprache der internationalen Anmeldung (nach Regel 48.3(b)).
- ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen vorläufigen Prüfung eingereicht worden ist (nach Regel 55.2 und/oder 55.3).

3. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale vorläufige Prüfung auf der Grundlage des Sequenzprotokolls durchgeführt worden, das:

- ☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.
- ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.
- ☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.
- ☐ Die Erklärung, daß die in computerlesbarer Form erfassten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

4. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/EP99/09981

- ☐ Beschreibung, Seiten:
☐ Ansprüche, Nr.:
☐ Zeichnungen, Blatt:

5. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)).

(Auf Ersatzblätter, die solche Änderungen enthalten, ist unter Punkt 1 hinzuweisen; sie sind diesem Bericht beizufügen).

6. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja: Ansprüche	1-30
	Nein: Ansprüche	
Erfinderische Tätigkeit (ET)	Ja: Ansprüche	1-30
	Nein: Ansprüche	
Gewerbliche Anwendbarkeit (GA)	Ja: Ansprüche	1-30
	Nein: Ansprüche	

2. Unterlagen und Erklärungen
siehe Beiblatt

**V. BEGRÜNDETE FESTSTELLUNG NACH ARTIKEL 35 (2) HINSICHTLICH DER NEUHEIT, DER
ERFINDERISCHEN TÄTIGKEIT UND DER GEWERBLICHEN ANWENDBARKEIT; UNTERLAGEN UND
ERKLÄRUNGEN ZUR STÜTZUNG DIESER FESTSTELLUNG**

ANSPRÜCHE 1, 17, 28 UND 29

1. Die Erfindung bezieht sich auf ein Verfahren (Anspruch 1) und eine Vorrichtung (Anspruch 28) zum Erzeugen eines verschlüsselten Multimediadatenstroms sowie auf ein Verfahren (Anspruch 17) und eine Vorrichtung (Anspruch 29) zum Entschlüsseln eines verschlüsselten Multimediadatenstroms, wobei der Multimediadatenstrom einen Anfangsblock und einen Nutzdatenblock mit verschlüsselten Nutzdaten aufweist.

Aus dem in der Beschreibungseinleitung genannten Stand der Technik (insbesondere Dokument DE 196 25 635 C1) ist es bekannt, Teile des Anfangsblocks (Bestimmungsdatenblocks) sowie zumindest Teile des Nutzdatenblocks mit unterschiedlichen Schlüsseln zu verschlüsseln, wobei insbesondere symmetrische Verschlüsselungsverfahren eingesetzt werden. Bei symmetrischen Verschlüsselungsverfahren benötigt der Benutzer, der die Datei entschlüsseln will, den gleichen Schlüssel wie der Provider oder Lieferant der die Multimediadaten verschlüsselt hat, um sie an den Kunden zu verkaufen.

Der vorliegenden Erfindung liegt die Aufgabe zugrunde, ein effizientes und sicheres Konzept zur Ver- bzw. Entschlüsselung von Multimediadaten zu schaffen.

Gelöst wird die Aufgabe durch die Verfahrensschritte der Ansprüche 1 und 17 und durch die Vorrichtungmerkmale der Ansprüche 28 und 29. Der vorliegenden Erfindung liegt die Erkenntnis zugrunde, daß zum sicheren und effizienten Verschlüsseln ein sogenanntes hybrides Verschlüsselungsverfahren eingesetzt werden muß, wobei das schnellere z.B. symmetrische Verschlüsselungsverfahren (Stand der Technik) oder Scramblingverfahren zum Ver- bzw. Entschlüsseln der Nutzdaten selbst, d.h. der "Payload"-Daten eingesetzt wird, während das langsamere asymmetrische Verschlüsselungskonzept nur verwendet wird, um den Nutzdatenschlüssel für das z.B. symmetrische Verschlüsselungskonzept zu verschlüsseln und in dieser verschlüsselten Form zu einem Benutzer zu übertragen, damit er den verschlüsselten Nutzdatenstrom wieder entschlüsseln

kann.

Das Anmeldungskonzept wird auch durch die im Internationalen Recherchenbericht genannte Druckschrift EP 0 438 154 A, die vom Anmeldungsgegenstand weiter weg liegt als der von der Anmelderin in der Beschreibung auf Seiten 1 bis 3 angegebene Stand der Technik, weder offenbart noch nahegelegt.

Der Gegenstand der Ansprüche 1, 17, 28 und 29 ist daher neu und erfinderisch (Artikel 33 (2) und (3) PCT).

2. Die abhängigen Ansprüche 2 bis 16 und 18 bis 27 enthalten weitere Details des Verfahrens zum Erzeugen eines verschlüsselten Multimediadatenstroms sowie des Verfahrens zum Entschlüsseln eines verschlüsselten Multimediadatenstroms gemäß Anspruch 1 bzw. 17. Der abhängige Anspruch 30 enthält weitere Details der Vorrichtung zum Erzeugen eines verschlüsselten Multimediadatenstroms sowie des Verfahrens zum Entschlüsseln eines verschlüsselten Multimediadatenstroms gemäß Anspruch 28 bzw. 29. Da die abhängige Ansprüche vom Anspruch 1, 17, 28 bzw. 29 abhängig sind, erfüllen auch sie die Erfordernisse gemäß PCT (Artikel 33 (2) und (3)) bezüglich Neuheit und erfinderischer Tätigkeit.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference FH991202.PCT	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/EP99/09981	International filing date (day/month/year) 15 December 1999 (15.12.99)	Priority date (day/month/year) 16 February 1999 (16.02.99)
International Patent Classification (IPC) or national classification and IPC H04L 9/00, H04N 7/167		
Applicant FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E.V.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of _____ sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand 13 September 2000 (13.09.00)	Date of completion of this report 30 January 2001 (30.01.2001)
Name and mailing address of the IPEA/EP	Authorized officer
Facsimile No.	Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/EP99/09981

I. Basis of the report

1. With regard to the elements of the international application:*

- ☐ the international application as originally filed
- ☒ the description:
 pages _____ 1-20 _____, as originally filed
 pages _____, filed with the demand
 pages _____, filed with the letter of _____
- ☒ the claims:
 pages _____ 1-30 _____, as originally filed
 pages _____, as amended (together with any statement under Article 19
 pages _____, filed with the demand
 pages _____, filed with the letter of _____
- ☒ the drawings:
 pages _____ 1/4-4/4 _____, as originally filed
 pages _____, filed with the demand
 pages _____, filed with the letter of _____
- ☐ the sequence listing part of the description:
 pages _____, as originally filed
 pages _____, filed with the demand
 pages _____, filed with the letter of _____

2. With regard to the language, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language _____ which is:

- ☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

- ☐ the description, pages _____
- ☐ the claims, Nos. _____
- ☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).

** Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

international application No.

PCT/EP 99/09981

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-30	YES
	Claims		NO
Inventive step (IS)	Claims	1-30	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-30	YES
	Claims		NO

2. Citations and explanations

Claims 1, 17, 28 and 29

- The invention relates to a method (Claim 1) and a device (Claim 28) for generating an encrypted multimedia data stream, and to a method (Claim 17) and a device (Claim 29) for decrypting an encrypted multimedia data stream, said multimedia data stream having a header block and a user data block containing encrypted user data.

It is known from the prior art referred to in the introductory part of the description (in particular DE-C1-196 25 635) to encrypt parts of a header block (destination data block) with different encryption keys, particularly using symmetrical encryption methods. With symmetrical encryption, the user who wishes to decrypt a file needs to have the same encryption key as the provider or supplier who encrypted the multimedia data in order to be able to sell it to the customer.

The present invention addresses the problem of devising an efficient and safe way of encrypting and decrypting multimedia data.

The problem is solved by the method steps defined in Claims 1 and 17 and by the device features defined in Claims 28 and 29. The invention is based on the insight that in order to ensure safe and efficient encryption it is necessary to use a hybrid encryption method, whereby a faster encryption method such as

symmetrical encryption (prior art) or scrambling is used to encrypt and decrypt the actual user data or payload data, whilst a slower asymmetrical encryption method is used to encrypt only the user data encryption key for the (for example) symmetrical encryption method and to transmit it in the encrypted form to a user to enable him to decrypt the encrypted user data stream.

The concept behind the invention is not disclosed in or suggested by the prior art, including EP-A-0 438 154 (cited in the international search report), which is further removed from the subject matter of the present application than the prior art cited by the applicant on pages 1-3 of the description.

The subject matter of Claims 1, 17, 28 and 29 is therefore novel and inventive (PCT Article 33(2) and (3)).

2. Dependent Claims 2-16 and 18-27 define further details relating to the method for generating an encrypted multimedia data stream and to the method for decrypting an encrypted multimedia data stream as per Claims 1 and 17. Dependent Claim 30 defines further details relating to the device for generating an encrypted multimedia data stream and to the method for decrypting an encrypted multimedia data stream as per Claims 28 and 29. The dependent claims are dependent on Claims 1, 17, 28 and 29 and therefore also meet the requirements of novelty and inventive step (PCT Article 33(2) and (3)).

PCT-ANTRAG

Original (für EINREICHUNG) - gedruckt am 15.12.1999 11:16:19 AM

0	Vom Anmeldeamt auszufüllen	
0-1	Internationales Aktenzeichen.	
0-2	Internationales Anmeldedatum	
0-3	Name des Anmeldeamts und "PCT International Application"	
0-4	Formular - PCT/RO/101 PCT-Antrag	
0-4-1	erstellt durch Benutzung von	PCT-EASY Version 2.90 (aktualisiert 15.10.1999)
0-5	Antragssuchen Der Unterzeichnete beantragt, daß die vorliegende internationale Anmeldung nach dem Vertrag über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens behandelt wird	
0-6	(Vom Anmelder gewähltes) Anmeldeamt	Europäisches Patentamt (EPA) (RO/EP)
0-7	Aktenzeichen des Anmelders oder Anwalts	FH991202.PCT
I	Bezeichnung der Erfindung	VERFAHREN UND VORRICHTUNG ZUM ERZEUGEN EINES VERSCHLÜSSELTEN NUTZDATENSTROMS UND VERFAHREN UND VORRICHTUNG ZUM ENTSCHLÜSSELN EINES VERSCHLÜSSELTEN NUTZDATENSTROMS
II	Anmelder	
II-1	Diese Person ist	nur Anmelder
II-2	Anmelder für	Alle Bestimmungsstaaten mit Ausnahme von US
II-4	Name	FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E.V.
II-5	Anschrift:	Leonrodstraße 54 D-80636 München Deutschland
II-6	Staatsangehörigkeit (Staat)	DE
II-7	Sitz/Wohnsitz (Staat)	DE
III-1	Anmelder und/oder Erfinder	
III-1-1	Diese Person ist	Anmelder und Erfinder
III-1-2	Anmelder für	Nur US
III-1-4	Name (FAMILIENNAME, Vorname)	RUMP, Niels
III-1-5	Anschrift:	Brückenstraße 13 D-91056 Erlangen Deutschland
III-1-6	Staatsangehörigkeit (Staat)	DE
III-1-7	Sitz/Wohnsitz (Staat)	DE

PCT-ANTRAG

FH991202.PCT

Original (für EINREICHUNG) - gedruckt am 15.12.1999 11:16:19 AM

III-2	Anmelder und/oder Erfinder	
III-2-1	Diese Person ist	Anmelder und Erfinder
III-2-2	Anmelder für	Nur US
III-2-4	Name (FAMILIENNAME, Vorname)	KOLLER, Jürgen
III-2-5	Anschrift:	St. Johann 6/113 D-91054 Erlangen Deutschland
III-2-6	Staatsangehörigkeit (Staat)	DE
III-2-7	Sitz/Wohnsitz (Staat)	DE
III-3	Anmelder und/oder Erfinder	
III-3-1	Diese Person ist	Anmelder und Erfinder
III-3-2	Anmelder für	Nur US
III-3-4	Name (FAMILIENNAME, Vorname)	BRANDENBURG, Karlheinz
III-3-5	Anschrift:	Haagstraße 32 D-91054 Erlangen Deutschland
III-3-6	Staatsangehörigkeit (Staat)	DE
III-3-7	Sitz/Wohnsitz (Staat)	DE
IV-1	Anwalt oder gemeinsamer Vertreter; oder besondere Zustellanschrift Die unten bezeichnete Person ist/wird hiermit bestellt, um den (die) Anmelder vor den internationalen Behörden zu vertreten, und zwar als:	Anwalt
IV-1-1	Name (FAMILIENNAME, Vorname)	SCHOPPE, Fritz
IV-1-2	Anschrift:	SCHOPPE, ZIMMERMANN & STÖCKELER POSTFACH 71 08 67 D-81458 München Deutschland
IV-1-3	Telefonnr.	089/7904450
IV-1-4	Telefaxnr.	089/7902215
IV-1-5	e-mail	101345.3117@CompuServe.com
V	Bestimmung von Staaten	
V-1	Regionales Patent (andere Schutzrechtsarten oder Verfahren sind ggf. in Klammern nach der (den) betreffenden Bestimmung(en) angegeben)	EP: AT BE CH&LI CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE und jeder weitere Staat, der Mitgliedsstaat des Europäischen Patentübereinkommens und Vertragsstaat des PCT ist
V-2	Nationales Patent (andere Schutzrechtsarten oder Verfahren sind ggf. in Klammern nach der (den) betreffenden Bestimmung(en) angegeben)	JP KR US

PCT-ANTRAG

FH991202.PCT

Original (für EINREICHUNG) - gedruckt am 15.12.1999 11:16:19 AM

V-5	Erklärung bzgl. vorsorglicher Bestimmungen Zusätzlich zu den unter Punkten V-1, V-2 and V-3 vorgenommenen Bestimmungen nimmt der Anmelder nach Regel 4.9 Absatz b auch alle anderen nach dem PCT zulässigen Bestimmungen vor mit Ausnahme der nachstehend unter Punkt V-6 angegebenen Staaten. Der Anmelder erklärt, daß diese zusätzlichen Bestimmungen unter dem Vorbehalt einer Bestätigung stehen und jede zusätzliche Bestimmung, die vor Ablauf von 15 Monaten ab dem Prioritätsdatum nicht bestätigt wurde, nach Ablauf dieser Frist als vom Anmelder zurückgenommen gilt.		
V-6	Staaten, die von der Erklärung über vorsorgliche Bestimmungen ausgenommen werden	KEINE	
VI-1	Priorität einer früheren nationalen Anmeldung beansprucht		
VI-1-1	Anmeldedatum	16 Februar 1999 (16.02.1999)	
VI-1-2	Aktenzeichen	19906450.4	
VI-1-3	Staat	DE	
VII-1	Gewählte Internationale Recherchenbehörde	Europäisches Patentamt (EPA) (ISA/EP)	
VIII	Kontrollliste	Anzahl der Blätter	Elektronische Datei(en) beigefügt
VIII-1	Antrag	4	-
VIII-2	Beschreibung	20	-
VIII-3	Ansprüche	9	-
VIII-4	Zusammenfassung	1	fh991202.txt
VIII-5	Zeichnung(en)	4	-
VIII-7	INSGESAMT	38	
VIII-8	Beigefügte Unterlagen	Unterlage(n) in Papierform beigefügt	Elektronische Datei(en) beigefügt
VIII-8	Blatt für die Gebührenberechnung	✓	-
VIII-10	Kopie der allgemeinen Vollmacht	Aktenzeichen 17406	-
VIII-16	PCT-EASY-Diskette	-	Diskette
VIII-18	Nr. der Abb. der Zeichn., die mit der Zusammenf. veröffentlicht werden soll	4	
VIII-19	Sprache der Int. Anmeldung	Deutsch	
IX-1	Unterschrift des Anmelders oder Anwalts		
IX-1-1	Name (FAMILIENNAME, Vorname)	SCHÖPPE Fritz	

VOM ANMELDEAMT AUSZUFÜLLEN

10-1	Datum des tatsächlichen Eingangs dieser internationalen Anmeldung	
10-2	Zeichnung(en):	
10-2-1	Eingegangen	
10-2-2	Nicht eingegangen	

PCT-ANTRAG

FH991202.PCT

Original (für EINREICHUNG) - gedruckt am 15.12.1999 11:16:19 AM

10-3	Geändertes Eingangsdatum aufgrund nachträglich, jedoch fristgerecht eingeg. Unterlage(n) oder Zeichnung(en) zur Vervollständigung dieser Int. Anmeldung	
10-4	Datum des fristgerechten Eingangs der Berichtigung nach PCT Artikel 11(2)	
10-5	Internationale Recherchenbehörde	ISA/EP
10-6	Übermittlung des Recherchenexemplars bis zur Zahlung der Recherchegebühr aufgeschoben	

VOM INTERNATIONALEN BÜRO AUSZUFÜLLEN

11-1	Datum des Eingangs des Aktenexemplars beim Internationalen Büro	
------	---	--

**PCT (ANHANG - BLATT FÜR DIE
GEBÜHRENBERECHNUNG)**


Original (für EINREICHUNG) - gedruckt am 15.12.1999 11:16:19 AM

(Dieses Blatt zählt nicht als Blatt der internationalen Anmeldung und ist nicht Teil derselben)

0	Vom Anmeldeamt auszufüllen		
0-1	Internationales Aktenzeichen.		
0-2	Eingangsstempel des Anmeldeamts		
0-4	Formular - PCT/RO/101 (Anlage)		
0-4-1	PCT Blatt für die Gebührenberechnung erstellt durch Benutzung von	PCT-EASY Version 2.90 (aktualisiert 15.10.1999)	
0-9	Aktenzeichen des Anmelders oder Anwalts	FH991202.PCT	
2	Anmelder	FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E.V., et al.	
12	Berechnung der vorgeschriebenen Gebühren	Höhe der Gebühr/Multiplikator	Gesamtbeträge (EUR)
12-1	Übermittlungsgebühr T	⇒	102
12-2	Recherchegebühr S	⇒	945
12-3	Internationale Gebühr Grundgebühr (erste 30 Blätter) b1	413	
12-4	Anzahl der Blätter über 30	8	
12-5	Zusatzblattgebühr (X)	10	
12-6	Gesamtbetrag der weiteren Gebühren b2	80	
12-7	b1 + b2 = B	493	
12-8	Bestimmungsgebühren Anzahl der in der internationalen Anmeldung vorgenommenen Bestimmungen	4	
12-9	Anzahl der zu zahlenden Bestimmungsgebühren (höchstens 10)	4	
12-10	Bestimmungsgebühr (X)	95	
12-11	Gesamtbetrag der Bestimmungsgebühren D	380	
12-12	PCT-EASY-Gebührenermäßigu ng R	-127	
12-13	Gesamtbetrag der internationalen Gebühr (B+D-R) I	⇒	746
12-17	Gesamtbetrag der zu zahlenden Gebühren (T+S+I+P)	⇒	1.793
12-19	Zahlungsart	Abbuchungsauftrag	
12-20	Anweisungen betreffend laufendes Konto Das Anmeldeamt:	Europäisches Patentamt (EPA) (RO/EP)	
12-20-1	wird beauftragt, den vorstehend angegebenen Gesamtbetrag der Gebühren von meinem laufenden Konto abzubuchen	✓	

PCT (ANHANG - BLATT FÜR DIE GEBÜHRENBERECHNUNG)

Original (für EINREICHUNG) - gedruckt am 15.12.1999 11:16:19 AM

12-20-2	wird beauftragt, Fehlbeträge oder Überzahlungen des vorstehend angegebenen Gesamtbetrags der Gebühren meinem laufenden Konto zu belasten bzw. gutzuschreiben	✓
12-21	Nummer des laufenden Kontos	2800 0601
12-22	Datum	15 Dezember 1999 (15.12.1999)
12-23	Name und Unterschrift	SCHOPPE, Fritz 

PRÜFPROTOKOLL UND BEMERKUNGEN

13-2-1	Prüfergebnisse Antrag	Grün? Die Bezeichnung der Erfindung muß kurz und genau gefaßt sein. Bitte überprüfen.
13-2-2	Prüfergebnisse Staaten	Grün? Es können mehr Bestimmungen vorgenommen werden. Bitte überprüfen.
13-2-3	Prüfergebnisse Namen	Grün? Anmelder 1.: Telefonnr. nicht angegeben
		Grün? Anmelder 1.:Telefaxnr. nicht angegeben
13-2-6	Prüfergebnisse Inhalt	Grün? Priority 1: der Prioritätsbeleg ist nicht beigelegt (der Anmelder muß ihn beim Anmeldeamt oder beim Internationalen Büro vor Ablauf von 16 Monaten ab dem (frühesten) Prioritätsdatum einreichen)
13-2-8	Prüfergebnisse Zahlung	Grün? Bitte überprüfen Sie, daß bei dem gewählten Anmeldeamt ein gültiges laufendes Konto auf Ihren Namen besteht

Original (für EINREICHUNG) - gedruckt am 15.12.1999 11:16:19 AM

PCT-EASY-Informationsblatt

(Vom Anmelder auszufüllen; dieses Blatt NICHT mit der internationalen Anmeldung einreichen)

PRÜFPROTOKOLL

Antrag	
Grün?	Die Bezeichnung der Erfindung muß kurz und genau gefaßt sein. Bitte überprüfen.
Staaten	
Grün?	Es können mehr Bestimmungen vorgenommen werden. Bitte überprüfen.
Namen	
Grün?	Anmelder 1.: Telefonnr. nicht angegeben
Grün?	Anmelder 1.:Telefaxnr. nicht angegeben
Inhalt	
Grün?	Priority 1: der Prioritätsbeleg ist nicht beigelegt (der Anmelder muß ihn beim Anmeldeamt oder beim Internationalen Büro vor Ablauf von 16 Monaten ab dem (frühesten) Prioritätsdatum einreichen)
Zahlung	
Grün?	Bitte überprüfen Sie, daß bei dem gewählten Anmeldeamt ein gültiges laufendes Konto auf Ihren Namen besteht

Vor Einreichung der internationalen Anmeldung, bitte sorgfältig prüfen daß:

- die Angaben auf dem ausgedruckten Anmeldeformular sind richtig;
- Box IX of the Request form and Item 12-22 of the Annex to the Request form have been signed;
- alle in Feld Nr. VIII des Antragsformulars angegebenen Bestandteile der internationalen Anmeldung sind beigelegt; und,
- die Diskette mit der PCT-EASY-Zipdatei der internationalen Anmeldung ist beigelegt und eindeutig mit "PCT-EASY", dem Aktenzeichen des Anmelders/Anwalts und dem Familiennamen des Anmelders beschriftet

ACHTUNG

KEINE Angaben auf dem ausgedruckten Antragsformular verändern. Die beigelegte PCT-EASY-Anmeldung ist gesperrt. Falls jetzt ein Fehler oder eine Auslassung entdeckt wird, muß die eingereichte Anmeldung als Vorlage kopiert und die Änderung oder Berichtigung in einer neuen Anmeldung vorgenommen werden (unter Verwendung der Vorlage) Sie können eine solche Vorlage erstellen, indem Sie die eingereichte Anmeldung aus dem Ordner "Gespeicherte Formulare" in den Ordner "Neue PCT Formulare" kopieren. Neue, in dem Ordner "Neue PCT Formulare" erstellte (.eft) Datei öffnen, Berichtigungen vornehmen und das Einreichungsverfahren fortsetzen

Patentanwälte · Postfach 710867 · 81458 München
Fraunhofer-Gesellschaft
zur Förderung der
angewandten Forschung e. V.
Leonrodstraße 54
D-80636 München
DE

PATENTANWÄLTE

European Patent Attorneys
European Trademark Attorneys

Fritz Schoppe, Dipl.-Ing.
Tankred Zimmermann, Dipl.-Ing.
Ferdinand Stöckeler, Dipl.-Ing.

Telefon/Telephone 089/790445-0
Telefax/Facsimile 089/790 22 15
Telefax/Facsimile 089/74996977
e-mail 101345.3117@CompuServe.com

**Verfahren und Vorrichtung zum Erzeugen eines verschlüsselten
Nutzdatenstroms und Verfahren und Vorrichtung zum
Entschlüsseln eines verschlüsselten Nutzdatenstroms**

**Verfahren und Vorrichtung zum Erzeugen eines verschlüsselten
Nutzdatenstroms und Verfahren und Vorrichtung zum
Entschlüsseln eines verschlüsselten Nutzdatenstroms**

Beschreibung

Die vorliegende Erfindung bezieht sich auf die Verschlüsselung und Entschlüsselung von Nutzdaten und insbesondere auf ein Verschlüsselungskonzept, bei dem die Nutzdaten mittels eines bestimmten Schlüssels verschlüsselt sind, wobei dieser Schlüssel wiederum selbst verschlüsselt ist, um eine kundenselektive Übertragen von Nutzdaten zu verwirklichen.

Mit dem Auftreten von Telekommunikationsnetzen und insbesondere aufgrund der großen Verbreitung von Multimediatdaten-fähigen Personalcomputern und in letzter Zeit auch von sogenannten Solid-State-Playern, entstand ein Bedarf, digitale Multimediatdaten, wie z. B. digitale Audiodaten und/oder digitale Videodaten, kommerziell zu vertreiben. Die Telekommunikationsnetze können beispielsweise analoge Telephonleitungen, digitale Telephonleitungen, wie z. B. ISDN, oder auch das Internet sein. Unter kommerziellen Anbietern von Multimediatprodukten besteht der Bedarf, Multimediatdaten zu verkaufen oder auszuleihen, wobei es einem Kunden möglich sein sollte, aus einem bestimmten Katalog zu jeder Zeit individuell ein bestimmtes Produkt auswählen zu können, das dann selbstverständlich nur von dem Kunden, der dafür bezahlt hat, benutzt werden darf.

Im Gegensatz zu bekannten verschlüsselten Fernsehprogrammen, wie z. B. von dem Fernsehkanal Premiere, bei dem die ausgesendeten Daten für alle Benutzer, die gegen eine bestimmte Gebühr eine geeignete Entschlüsselungsvorrichtung erworben haben, gleich verschlüsselt sind, soll die vorliegende Erfindung Verfahren und Vorrichtungen schaffen, die eine individuelle, kundenselektive und sichere Verschlüsselung und

Entschlüsselung von Multimediatdaten ermöglichen. Im Gegensatz zu den genannten Fernsehkanälen, die ein festes Programm vorgeben, für das sich der Benutzer komplett entscheiden muß, ermöglichen die Verfahren und Vorrichtungen der vorliegenden Erfindung eine maximale Wahlfreiheit des Kunden, d. h. derselbe muß nur für die Produkte bezahlen, die er tatsächlich auch benutzen will.

Die DE 196 25 635 C1 beschreibt Verfahren und Vorrichtungen zum Ver- bzw. Entschlüsseln von Multimediatdaten, wobei die Multimediatdaten in Form einer verschlüsselten Multimediatdatei vorliegen, die einen Bestimmungsdatenblock und einen Nutzdatenblock aufweist. Teile des Bestimmungsdatenblocks sowie zumindest Teile des Nutzdatenblocks werden mit unterschiedlichen Schlüsseln verschlüsselt, wobei insbesondere symmetrische Verschlüsselungsverfahren eingesetzt werden.

Symmetrische Verschlüsselungsverfahren haben einerseits den Vorteil, daß sie relativ schnell arbeiten, andererseits benötigt der Benutzer, der die Datei entschlüsseln will, den gleichen Schlüssel wie der Provider oder Lieferant, z. B. die Deutsche Telekom, der die Multimediatdaten verschlüsselt hat, um sie an den Kunden zu verkaufen. Somit haben sowohl der Provider als auch der Benutzer, d. h. der Kunde, einerseits eine Tabelle mit vielen möglichen symmetrischen Verschlüsselungsalgorithmen, wie z. B. DES oder Blowfish, und andererseits eine Tabelle für mögliche Schlüssel, derart, daß vom Provider ein Eintrag in dem Bestimmungsdatenblock der Multimediatdaten erzeugt wird, den der Benutzer verwendet, um damit auf seine Schlüsseltabelle zuzugreifen, um den korrekten Schlüssel zum Entschlüsseln auszuwählen.

Aufgrund der stark zunehmenden Verbreitung des MP3-Standards sind auf dem Markt sogenannten Solid-State-Player erschienen, die zum Entschlüsseln und Abspielen von Multimediatdaten eingesetzt werden sollen. Diese Geräte sollen sehr preisgünstig sein und dürfen daher lediglich eine begrenzte Menge an Speicherplatz und Rechenleistung haben. Im Gegensatz zu

Personalcomputern, bei denen die vorhandenen Ressourcen die für die Entschlüsselung von Multimediatdaten benötigten Ressourcen bei weitem übersteigen, müssen Solid-State-Player oder Stereoanlagen oder Auto-HiFi-Geräte, damit sie sich auf dem hart umkämpften Markt durchsetzen können, preiswert sein. Dazu ist es erforderlich, diese Geräte beim Entschlüsseln und Abspielen der entschlüsselten Multimediatdaten soweit als möglich bezüglich Rechenleistung und Speicherplatz zu entlasten. Andererseits besteht nach wie vor die Anforderung, daß die verwendeten Verschlüsselungstechniken ausreichend sicher sind, um für einen Kunden vertrauenswürdig zu sein, und um einen Mißbrauch auch verschlüsselter Multimediatdaten zu vermeiden. Weiterhin gilt es, wirksam Urheberrechtsverletzungen zu begegnen, insbesondere, wenn Multimediatdaten ohne Autorisierung durch den Urheber bzw. eine Verwertungsgesellschaft abgespielt werden, oder auch ohne Autorisierung verändert werden.

Die Aufgabe der vorliegenden Erfindung besteht darin, ein effizientes und sicheres Konzept zur Ver- bzw. Entschlüsselung von Multimediatdaten zu schaffen.

Diese Aufgabe wird durch ein Verfahren zum Erzeugen eines verschlüsselten Multimediatdatenstroms nach Anspruch 1, durch ein Verfahren zum Entschlüsseln eines verschlüsselten Multimediatdatenstroms nach Anspruch 17, durch eine Vorrichtung zum Erzeugen eines verschlüsselten Multimediatdatenstroms nach Anspruch 27 und durch eine Vorrichtung zum Entschlüsseln eines verschlüsselten Multimediatdatenstroms nach Anspruch 28 gelöst.

Der vorliegenden Erfindung liegt die Erkenntnis zugrunde, daß zum sicheren und effizienten Verschlüsseln ein sogenanntes hybrides Verschlüsselungsverfahren eingesetzt werden muß, wobei das schnellere z. B. symmetrische Verschlüsselungsverfahren oder Scramblingverfahren zum Ver- bzw. Entschlüsseln der Nutzdaten selbst, d. h. der "Payload"-Daten, eingesetzt wird, während das langsamere asymmetrische Ver-

schlüsselungskonzept nur verwendet wird, um den Nutzdaten-Schlüssel für das z. B. symmetrische Verschlüsselungskonzept zu verschlüsseln und in dieser verschlüsselten Form zu einem Benutzer zu übertragen, damit er den verschlüsselten Nutzdatenstrom wieder entschlüsseln kann. Weiterhin soll der verschlüsselte Nutzdatenstrom, der einerseits eine Nutzdatei sein könnte oder aber ein durchgehender Datenstrom sein kann, gegen unerlaubte Manipulationen gesichert werden. Um dies auf effiziente und möglichst Rechenzeit-sparende Art und Weise zu verwirklichen, wird in das asymmetrische Verschlüsselungsverfahren zum Verschlüsseln des Nutzdaten-Schlüssels der Nutzdatenstrom selbst mit einbezogen.

An dieser Stelle sei darauf hingewiesen, daß Nutzdaten allgemein Multimediadaten, d. h. Audiodaten, Videodaten oder eine Kombination aus Audiodaten und Videodaten, aber auch z. B. Textdaten und sogar Binärdaten, wie z. B. ausführbare Programme, umfassen. Im nachfolgenden wird der Gegenstand der vorliegenden Erfindung aus Zweckmäßigkeitsgründen jedoch anhand von Multimediadaten dargelegt. Es ist jedoch offensichtlich, daß sämtliche Nutzdaten, für die es ein Verschlüsselungsinteresse gibt, durch die erfindungsgemäßen Vorrichtungen und Verfahren verarbeitet werden können.

Vorzugsweise wird eine Hash-Summe eines Teils des Multimediadatenstroms erzeugt. Dieser Teil könnte zum einen lediglich der Anfangsblock des Multimediadatenstroms sein, zum anderen aber auch Teile der verschlüsselten bzw. unverschlüsselten Multimediadaten selbst umfassen.

Ein Ausgabewert in dem Anfangsblock, der dem Kunden zusammen mit den zumindest teilweise verschlüsselten Multimediadaten in Form des Multimediadatenstroms übermittelt wird, stellt gewissermaßen eine verschlüsselte Version des Multimediadaten-Schlüssels dar, wobei, um diesen Ausgabewert wieder korrekt zu entschlüsseln, um den Multimediadaten-Schlüssel zu erhalten, neben dem Schlüssel für das asymmetrische Verschlüsselungsverfahren auch vom Provider erzeugte indivi-

duelle Daten, wie z. B. Lizenzdaten, die sich auf die Art und Weise beziehen, wie ein Benutzer die verschlüsselten Multimediadaten überhaupt benutzen darf, als auch Teile der Multimediadaten selbst sein können. Führt ein Benutzer daher Manipulationen an dem Anfangsblock durch, indem er beispielsweise das Verfallsdatum seiner Lizenz, ein bestimmtes Multimediastück zu verwenden, verändert, so kann er keinesfalls mehr den korrekten Schlüssel zum Entschlüsseln der verschlüsselten Multimediadaten ermitteln, da keine korrekte Entschlüsselung des Ausgabewerts mehr möglich ist.

Ein wesentlicher Vorteil des Verfahrens besteht also darin, daß, sobald jemand den Anfangsblock verändert, sich auch die Hash-Summe über den Anfangsblock ändert. Dadurch ist es nicht mehr möglich, den Schlüssel zum Entschlüsseln der Multimediadaten korrekt zu ermitteln. Somit führt jegliche Änderung am Anfangsblock automatisch zur Zerstörung der Multimediadaten selber.

Diese "implizite" Sicherung des Anfangsblocks umfaßt keine Verschlüsselung des Anfangsblocks, weshalb derselbe auch nicht entschlüsselt werden muß, was bei den Abspielvorrichtungen wiederum zu Ressourceneinsparungen ausgenutzt werden kann. Natürlich wäre eine solche Verschlüsselung des Anfangsblocks ohne weiteres möglich, wenn der Wunsch danach besteht.

Analog dazu führt, wenn verschlüsselte oder unverschlüsselte Multimediadaten selbst in die Verschlüsselung des Multimediadaten-Schlüssels mit einbezogen werden, eine Veränderung an den Multimediadaten zu einer automatischen Zerstörung der gesamten Multimediadaten.

Bevorzugte Ausführungsbeispiele der vorliegenden Erfindung werden nachfolgend bezugnehmend auf die beiliegenden Zeichnungen detailliert erläutert. Es zeigen:

Fig. 1 einen Multimediadaten-Strom, der gemäß der vorlie-

genden Erfindung erzeugt werden kann;

- Fig. 2 eine detailliertere Darstellung des Anfangsblocks und des Nutzdatenblocks des verschlüsselten Multimediadatenstroms;
- Fig. 3 eine Auswahl bestimmter Einträge in die einzelnen Unterblöcke des Anfangsblocks;
- Fig. 4 ein Flußdiagramm für das Verfahren zum Erzeugen eines verschlüsselten Multimediadatenstroms gemäß der vorliegenden Erfindung, das vorzugsweise bei einem Distributor, d. h. einem Lieferanten, von Multimediadaten ausgeführt wird; und
- Fig. 5 ein Verfahren zum Entschlüsseln eines verschlüsselten Multimediadatenstroms gemäß der vorliegenden Erfindung, das vorzugsweise bei einem Kunden oder Benutzer der Multimediadaten ausgeführt wird.

Fig. 1 zeigt einen verschlüsselten Multimediadatenstrom 10, der einen Anfangsblock oder Header 12 und einen Nutzdatenblock 14, d. h. einen Block mit verschlüsselten Multimediadaten, aufweist. Der Nutzdatenblock 14 umfaßt verschlüsselte Abschnitte 16 und unverschlüsselte Abschnitte 18 zwischen den verschlüsselten Abschnitten 16. Außerdem umfaßt ein Multimediadatenstrom, der gemäß der vorliegenden Erfindung erzeugt werden kann, einen weiteren unverschlüsselten Abschnitt 20, der auf den Anfangsblock 12 folgt und vor einem verschlüsselten Abschnitt 16 angeordnet ist.

Üblicherweise sind die zu verschlüsselten Multimediadaten auf irgendeine Art und Weise codiert, wie z. B. nach einem MPEG-Standard, wie z. B. MPEG-2 AAC, MPEG-4 Audio oder MPEG Layer-3. Daher ist es ausreichend, gewisse Abschnitte der zu verschlüsselten Multimediadaten zu verschlüsseln. Dies führt zu einem wesentlich verringerten Verarbeitungsaufwand sowohl beim Provider, der die Daten verschlüsselt, als auch beim

Kunden, der die Daten wieder entschlüsseln muß. Außerdem wird durch die lediglich teilweise Verschlüsselung der Multimediatdaten der Hörgenuß bzw. der Sehgenuß eines Benutzers, der lediglich die unverschlüsselten Multimediatdaten verwendet, durch die ständig auftretenden verschlüsselten Blöcke stark beeinträchtigt.

Obwohl Fig. 1 einen verschlüsselten Multimediatdatenstrom zeigt, bei dem der Anfangsblock 12 am Anfang des verschlüsselten Multimediatdatenstroms angeordnet ist, soll sich diese Anordnung von Anfangsblock und Nutzdatenblock nicht auf die Übertragung des verschlüsselten Multimediatdatenstroms beziehen. Der Ausdruck "Anfangsblock" soll lediglich zum Ausdruck bringen, daß eine Entschlüsselungsvorrichtung, die den verschlüsselten Multimediatdatenstrom entschlüsseln möchte, zunächst zumindest Teile des Anfangsblocks benötigt, bevor die Multimediatdaten selbst entschlüsselt werden können. Je nach Übertragungsmedium könnte der Anfangsblock irgendwo auch innerhalb des Nutzdatenblocks angeordnet sein bzw. durchaus nach bestimmten Teilen des Nutzdatenblocks empfangen werden, wenn beispielsweise an eine Paket-orientierte Übertragung des Multimediatdatenstroms gedacht wird, bei der unterschiedliche Pakete, von denen eines den Anfangsblock enthalten kann und ein anderes einen Teil des Nutzdatenblocks enthalten kann, über unterschiedliche physische Übertragungswege übertragen werden, derart, daß die Empfangsreihenfolge ganz und gar nicht der Sendereihenfolge entsprechen muß. Eine Entschlüsselungsvorrichtung muß in diesem Fall jedoch in der Lage sein, die empfangenen Pakete zu speichern und wieder zu ordnen, derart, daß Informationen aus dem Anfangsblock extrahiert werden, um mit dem Entschlüsseln zu beginnen. Der verschlüsselte Multimediatdatenstrom könnte ferner in Form einer Datei vorliegen oder aber auch in Form eines tatsächlichen Datenstroms, wenn beispielsweise an eine Live-Übertragung eines Multimediaereignisses gedacht wird. Diese Anwendung wird insbesondere beim digitalen Benutzer-selektiven Rundfunk auftreten.

Die Länge eines verschlüsselten Abschnitts 16 wird durch einen Wert Menge 22 dargestellt, während der Abstand im verschlüsselten Multimediateststrom von dem Beginn eines verschlüsselten Abschnitts 16 bis zum Beginn des nächsten verschlüsselten Abschnitts 16 mit Schritt 24 bezeichnet wird. Die Länge des weiteren verschlüsselten Abschnitts 20 wird durch einen Wert Erster Schritt 26 angegeben.

Diese Werte 22, 24 und 26 werden selbstverständlich für ein korrektes Entschlüsseln der Multimediatestdaten in einer Entschlüsselungsvorrichtung benötigt, weshalb dieselben in den Anfangsblock 12 eingetragen werden müssen, wie es später erläutert wird.

Fig. 2 zeigt eine detailliertere Darstellung des verschlüsselten Multimediateststroms 10, der aus dem Anfangsblock 12 und dem Nutzdatenblock 14 besteht. Der Anfangsblock 12 ist in mehrere Unterblöcke unterteilt, die im einzelnen insbesondere bezugnehmend auf Fig. 3 erläutert werden. Es sei darauf hingewiesen, daß die Anzahl und Funktion der Unterblöcke beliebig erweitert werden kann. In Fig. 2 sind daher lediglich beispielhaft einzelne Unterblöcke des Anfangsblocks 12 aufgeführt. Derselbe umfaßt, wie es in Fig. 2 gezeigt ist, einen sogenannten Crypt-Block 29, der allgemein gesagt für das Verschlüsseln der Multimediatestdaten relevante Informationen aufweist. Weiterhin umfaßt der Anfangsblock 12 einen sogenannten Lizenz-Block 30, der Daten aufweist, die sich auf die Art und Weise beziehen, wie ein Benutzer den verschlüsselten Multimediateststrom verwenden kann bzw. darf. Der Anfangsblock 12 umfaßt ferner einen Nutzdateninfo-Block 32, der Informationen bezüglich des Nutzdatenblocks 14 sowie generelle Informationen über den Anfangsblock 12 selbst umfassen kann. Weiterhin kann der Anfangsblock 12 einen Alter-Anfangsblock-Block 34 aufweisen, der eine sogenannte rekursive Anfangsblock-Struktur ermöglicht. Dieser Block versetzt den Benutzer, der neben einer Entschlüsselungsvorrichtung auch eine Verschlüsselungsvorrichtung hat, in die Lage, einen verschlüsselten Multimediateststrom für

andere in seinem Besitz befindliche Abspielgeräte umzuformieren, ohne die ursprünglichen vom Distributor gelieferten Anfangsblockinformationen zu verlieren bzw. zu modifizieren. Je nach Anwendungsbereich können noch weitere Unterblöcke, wie z. B. ein IP-Information-Block (IP = Intellectual Property = Geistiges Eigentum) nach ISO/IEC 14496-1, MPEG-4, Systems, 1998, der Urheberrechtsinformationen umfaßt, zu dem Anfangsblock 12 hinzugefügt werden.

Wie es in der Technik üblich ist, kann jedem Block eine interne Blockstruktur zugewiesen werden, die zunächst einen Blockidentifikator fordert, die dann die Länge des Unterblocks umfaßt, und die dann schließlich die Block-Nutzdaten selbst aufführt. Damit erhält der verschlüsselte MultimediaDatenstrom und insbesondere der Anfangsblock des verschlüsselten MultimediaDatenstroms einer erhöhte Flexibilität, derart, daß auf neue Anforderungen insoweit reagiert werden kann, daß zusätzliche Unterblöcke hinzugefügt werden bzw. bestehende Unterblöcke weggelassen werden können.

Fig. 3 gibt eine Übersicht über die Block-Nutzdaten der einzelnen in Fig. 2 dargestellten Unterblöcke.

Zunächst wird auf den Crypt-Block 28 eingegangen. Derselbe enthält einen Eintrag für einen MultimediaDaten-Verschlüsselungsalgorithmus 40, der den bei einem bevorzugten Ausführungsbeispiel verwendeten symmetrischen Verschlüsselungsalgorithmus identifiziert, der beim Verschlüsseln der MultimediaDaten verwendet worden ist. Der Eintrag 40 dürfte ein Index für eine Tabelle sein, derart, daß eine Entschlüsselungsvorrichtung nach Lesen des Eintrags 40 in der Lage ist, denselben Verschlüsselungsalgorithmus aus einer Vielzahl von Verschlüsselungsalgorithmen auszuwählen, den die Verschlüsselungsvorrichtung verwendet hat. Der Crypt-Block 28 umfaßt ferner den Eintrag Erster Schritt 26, den Eintrag Schritt 24 und den Eintrag Menge 22, die bereits in Verbindung mit Fig. 1 dargestellt worden sind. Diese Einträge in dem Anfangsblock versetzen eine Entschlüsselungsvorrichtung in die

Lage, einen verschlüsselten Multimediatatenstrom entsprechend unterzugliedern, um eine korrekte Entschlüsselung durchführen zu können.

Der Crypt-Block 28 enthält ferner einen Eintrag für den Distributor bzw. Provider bzw. Lieferanten 42, der ein Code für den Distributor ist, der den verschlüsselten Multimediatatenstrom erzeugt hat. Ein Eintrag Benutzer 44 identifiziert den Benutzer, der von dem Distributor, der durch den Eintrag 42 identifiziert ist, den verschlüsselten Multimediatatenstrom auf irgendeine Art und Weise erhalten hat. Eine mögliche Verwendung dieser Kennungen ist es, die Benutzererkennung gerätespezifisch durchzuführen. Der Eintrag Benutzer würde dann die Seriennummer eines PC, eines Laptops, eines Auto-HiFi-Geräts, einer Heim-Stereoanlage etc. umfassen, die ein Abspielen nur auf dem speziellen Gerät zuläßt. Zur weiteren Erhöhung der Flexibilität und/oder Sicherheit könnte statt der Seriennummer, die bei jedem Hersteller unterschiedlich aussieht, die aber zufällig identisch sein könnten, eine spezielle Kennung, wie z. B. eine logische Verknüpfung der Festplattengröße mit der Prozessornummer etc. beim Beispiel eines PC, eingesetzt werden.

Ein Eintrag 46 enthält einen Ausgabewert, auf den später detailliert eingegangen wird. Dieser Ausgabewert stellt allgemein gesagt eine verschlüsselte Version des Multimediataten-Schlüssels dar, der in Verbindung mit dem durch den Eintrag 40 identifizierten Multimediataten-Verschlüsselungsalgorithmus benötigt wird, um die in dem Nutzdatenblock 14 vorhandenen verschlüsselten Multimediataten (Abschnitte 16 von Fig. 1) korrekt zu entschlüsseln. Um eine ausreichende Flexibilität für zukünftige Anwendungen zu haben, sind ferner die beiden Einträge Ausgabewertlänge 48 und Ausgabewertmaske 50 vorgesehen. Der Eintrag Ausgabewertlänge 48 gibt an, welche Länge der Ausgabewert 46 tatsächlich hat. Um ein flexibles Anfangsblockformat zu erhalten, sind jedoch in dem Anfangsblockformat für den Ausgabewert mehr Byte vorge-

sehen als ein Ausgabewert derzeit tatsächlich hat. Die Ausgabewertmaske 50 gibt daher an, wie ein kürzerer Ausgabewert auf einen längeren Ausgabewertplatz gewissermaßen verteilt wird. Ist die Ausgabewertlänge beispielsweise halb so groß wie der verfügbare Platz für den Ausgabewert, so könnte die Ausgabewertmaske derart gestaltet sein, daß die erste Hälfte der Ausgabewertmaske gesetzt ist, während die zweite Hälfte abgedeckt ist. Dann würde der Ausgabewert einfach in den von der Syntax für den Anfangsblock vorgesehenen Raum eingetragen werden und die erste Hälfte einnehmen, während die andere Hälfte aufgrund der Ausgabewertmaske 50 ignoriert wird.

Im nachfolgenden wird auf den Lizenz-Block 30 des Anfangsblocks 12 eingegangen. Derselbe umfaßt einen Eintrag Bitmaske 52. Dieser Eintrag kann bestimmte spezielle Informationen für das Abspielen bzw. für die generelle Art der Verwendung der verschlüsselten Multimediatdaten haben. Insbesondere könnte hiermit einer Entschlüsselungsvorrichtung mitgeteilt werden, ob bzw. ob nicht die Nutzdaten lokal abgespielt werden können. Weiterhin könnte hier signalisiert werden, ob das Herausforderungs-Antwort-Verfahren zum Verschlüsseln eingesetzt worden ist, das in dem eingangs erwähnten Deutschen Patent DE 196 25 635 C1 beschrieben ist und einen effizienten Datenbankzugriff ermöglicht.

Ein Eintrag Verfallsdatum 54 gibt den Zeitpunkt an, zu dem die Erlaubnis, den verschlüsselten Multimediatdatenstrom zu entschlüsseln, erlischt. Eine Entschlüsselungsvorrichtung wird in diesem Fall den Eintrag Verfallsdatum 54 prüfen und mit einer eingebauten Zeitmeßeinrichtung vergleichen, um im Falle, daß das Verfallsdatum bereits überschritten ist, keine Entschlüsselung des verschlüsselten Multimediatdatenstroms mehr durchzuführen. Dies erlaubt es einem Provider, auch zeitlich begrenzt verschlüsselte Multimediatdaten zur Verfügung zu stellen, was den Vorteil einer wesentlich flexibleren Handhabung und auch Preisgestaltung ermöglicht. Diese Flexibilität wird weiter durch einen Eintrag Anfangsdatum 56

unterstützt, in dem spezifiziert ist, ab wann eine verschlüsselte Multimediadatei entschlüsselt werden darf. Eine Verschlüsselungsvorrichtung wird den Eintrag Anfangsdatum mit ihrer eingebauten Uhr vergleichen, um erst dann eine Entschlüsselung der verschlüsselten Multimediadaten durchzuführen, wenn der aktuelle Zeitpunkt später als das Anfangsdatum 56 ist.

Ein Eintrag Erlaubte Abspielanzahl 58 gibt an, wie oft der verschlüsselte Multimediadatenstrom entschlüsselt, d. h. abgespielt werden darf. Dies erhöht weiter die Flexibilität des Providers, derart, daß er nur eine bestimmte Anzahl des Abspielens beispielsweise gegen eine bestimmte Summe zuläßt, die kleiner ist als eine Summe, die für die unbeschränkte Nutzung des verschlüsselten Multimediadatenstroms anfallen würde.

Zur Verifizierung bzw. Unterstützung des Eintrags Erlaubte Abspielanzahl 58 umfaßt der Lizenz-Block 30 ferner einen Eintrag Tatsächliche Abspielanzahl 60, der nach jedem Entschlüsseln des verschlüsselten Multimediadatenstroms beispielsweise um Eins inkrementiert werden könnte. Eine Entschlüsselungsvorrichtung wird daher immer überprüfen, ob der Eintrag Tatsächliche Abspielanzahl kleiner als der Eintrag Erlaubte Abspielanzahl ist. Wenn dies der Fall ist, wird eine Entschlüsselung der Multimediadaten durchgeführt. Wenn dies nicht der Fall ist, wird keine Entschlüsselung mehr ausgeführt.

Analog zu den Einträgen 58 und 60 sind die Einträge Erlaubte Kopieanzahl 62 und Tatsächliche Kopieanzahl 64 implementiert. Durch die beiden Einträge 62 und 64 wird sichergestellt, daß ein Benutzer der Multimediadaten dieselben lediglich so oft kopiert, wie es ihm vom Provider erlaubt wird, bzw. so oft, wie er beim Kauf der Multimediadaten bezahlt hat. Durch die Einträge 58 bis 64 wird ein effektiver Urheberrechtsschutz sichergestellt, und kann eine Selektion zwischen privaten Nutzern und gewerblichen Nutzern

erreicht werden, beispielsweise, indem die Einträge Erlaubte Abspielanzahl 58 und Erlaubte Kopieanzahl 62 auf einen kleinen Wert eingestellt werden.

Die Lizenzierung könnte z. B. so gestaltet sein, daß eine bestimmte Anzahl von Kopien (Eintrag 62) des Originals erlaubt ist, während keine Kopien einer Kopie zulässig sind. Der Anfangsblock einer Kopie würde dann im Gegensatz zum Anfangsblock des Originals als Eintrag Erlaubte Kopieanzahl eine Null haben, derart, daß diese Kopie von einer ordnungsgemäßen Ver/Entschlüsselungsvorrichtung nicht mehr kopiert wird.

Bei dem hier gezeigten Beispiel für ein Multimediadatenschutzprotokoll (MMP; MMP = Multimedia Protection Protocol) enthält der Anfangsblock 12 ferner einen Nutzdaten-Informationsblock 32, der hier lediglich zwei Block-Nutzdateneinträge 66 und 68 hat, wobei der Eintrag 66 eine Hash-Summe über den gesamten Anfangsblock enthält, während der Eintrag 68 den Typ des Hash-Algorithmus identifiziert, der zum Bilden der Hash-Summe über den gesamten Anfangsblock verwendet worden ist.

In diesem Zusammenhang sei beispielsweise auf das Fachbuch "Applied Cryptography", Second Edition, John Wiley & Sons, Inc. von Bruce Schneier (ISBN 0 471-11709-9) verwiesen, das eine ausführliche Darstellung symmetrischer Verschlüsselungsalgorithmen, asymmetrischer Verschlüsselungsalgorithmen und Hash-Algorithmen umfaßt.

Der Anfangsblock 12 umfaßt schließlich den Alter-Anfangsblock-Block 34, der neben den Synchronisationsinformationen, die in Fig. 3 nicht dargestellt sind, den Eintrag Alter Anfangsblock 70 aufweist. In den Eintrag Alter-Anfangsblock 70 kann, wenn ein Benutzer selbst eine Verschlüsselung durchführt und somit einen neuen Anfangsblock 12 erzeugt, der alte Anfangsblock vom Provider bewahrt werden, um keine wesentlichen Informationen zu verlieren, die der Provider in

den Anfangsblock eingetragen hat. Dazu könnten beispielsweise Urheberinformationen (IP-Information-Block) frühere Benutzerinformationen und Distributoreninformationen zählen, die eine Zurückverfolgung einer Multimediatei, die beispielsweise mehrmals von unterschiedlichen Geräten ent-/ver-schlüsselt worden ist, auf den ursprünglichen Anbieter transparent ermöglichen, wobei Urheberinformationen bewahrt werden. Damit ist es möglich, jederzeit zu überprüfen, ob eine verschlüsselte Multimediatei legal oder illegal erworben worden ist.

Nachdem auf das Format des verschlüsselten Multimediatei-Stroms und verschiedene Funktionalitäten von Verschlüsselungs- und Entschlüsselungsvorrichtungen eingegangen worden ist, wird nun anhand von Fig. 4 das erfindungsgemäße Verfahren zum Verschlüsseln von Multimediatei dargelegt. Bei einer bevorzugten Anwendung der vorliegenden Erfindung wird das erfindungsgemäße Verschlüsselungsverfahren beim Distributor ausgeführt. Der Distributor führt bevorzugterweise ein hybrides Verschlüsselungsverfahren aus, d. h. ein symmetrisches Verschlüsselungsverfahren zum Verschlüsseln der Multimediatei und ein asymmetrisches Verschlüsselungsverfahren zum Verschlüsseln des Multimediatei-Schlüssels.

Ein Kunde oder Benutzer, der Multimediatei von einem Distributor erwerben will, tritt zunächst mit dem Distributor in Verbindung und könnte ihm beispielsweise seine Kreditkartennummer mitteilen, von der der Distributor fällige Geldbeträge abbucht. Daraufhin erhält der Kunde vom Distributor eine Tabelle der symmetrischen Verschlüsselungsverfahren. Außerdem tauschen Distributor und Kunde jeweils ihre öffentlichen Schlüssel aus. Wenn der Benutzer nun ein bestimmtes Multimediateiwerk vom Distributor bestellt, so führt der Distributor eine kundenselektive Verschlüsselung für diesen Kunden durch.

Im einzelnen könnten die Schritte zum Erzeugen des verschlüsselten Multimediatei-Stroms folgendermaßen aussehen.

Der Distributor erstellt zunächst den Anfangsblock 12 für die Multimediadatei soweit es bisher möglich ist (100). Wie es aus Fig. 3 ersichtlich ist, liegt zu diesem Zeitpunkt noch nicht der Ausgabewert vor. Daher wird im Schritt 100, in dem der Anfangsblock 12 soweit als möglich erstellt wird, der Eintrag für den Ausgabewert freigelassen. Es existieren jedoch hier schon sämtliche anderen Einträge in den Crypt-Block und sämtliche anderen Einträge in den Lizenz-Block. Die Hash-Summe oder je nach dem die digitale Unterschrift in dem Eintrag 66 über den gesamten Anfangsblock existiert dagegen noch nicht, weshalb auch dieser Eintrag frei bleibt. Auch der Eintrag Alter-Anfangsblock 70 wird sehr wahrscheinlich, wenn die Multimediadatei vom Distributor zum ersten Mal verschlüsselt werden, frei bleiben. Hat der Distributor die verschlüsselte Multimediadatei jedoch von einem anderen Distributor erworben, so könnte der Eintrag 70 bereits gefüllt sein. In einem Schritt 102 ermittelt der Distributor einen Multimediadatenschlüssel K, der zusammen mit dem Multimediadaten-Verschlüsselungsalgorithmus, der durch den Eintrag 40 (Fig. 3) identifiziert ist, eine Verschlüsselung der Multimediadaten erlaubt, die in einem Schritt 104 durchgeführt wird.

Gemäß der vorliegenden Erfindung wird eine Hash-Summe über den Anfangsblock gebildet, wobei bestimmte Teile einen vordefinierten Wert haben (Schritt 106). Die detaillierte Darstellung des Anfangsblocks in Fig. 3 enthält am rechten Rand eine Spalte 107, die veranschaulichen soll, welche Teile bzw. Einträge in den Anfangsblock 12 beim Bilden einer Hash-Summe im Schritt 106 (Fig. 4) einen vordefinierten Wert erhalten. Einen vordefinierten Wert erhalten insbesondere der Eintrag Ausgabewert 46, der Eintrag Tatsächliche Abspielanzahl 60, der Eintrag Tatsächliche Kopieanzahl 64 und der Eintrag Hash-Summe über den Anfangsblock 66 sowie unter Umständen der Eintrag Alter-Anfangsblock 70, wie es durch das gepunktete Kreuzchen für den Eintrag 70 dargestellt ist. Bestimmte Teile des Anfangsblocks müssen einen vordefinierten Wert zugewiesen bekommen, wenn die Hash-Summe im Schritt

106 gebildet wird, da diese noch nicht feststehen (Ausgabewert 46) bzw. von einer Entschlüsselungsvorrichtung geändert werden (Einträge 60 und 64). Der Eintrag 66, d. h. die Hash-Summe über den Anfangsblock, steht ferner noch nicht fest, da in dieselbe selbstverständlich auch der Ausgabewert 46 eingeht.

Die Einträge Distributor 42, Benutzer 44 sowie die Einträge in den Lizenz-Block 30 werden jedoch beim Bilden der Hash-Summe im Schritt 106 (Fig. 4) mit einbezogen, wodurch bereits eine Personalisierung bzw. eine Absicherung der Lizenz-Block-Einträge erreicht wird, da die in dem Schritt 106 erhaltene Hash-Summe mit dem Multimediataten-Schlüssel verknüpft wird, um einen Basiswert zu erhalten (Schritt 108).

Daran anschließend wird der im Schritt 108 erhaltene Basiswert mittels des öffentlichen Schlüssels (Ö) des Kunden asymmetrisch verschlüsselt (Schritt 110). Um den verschlüsselten Multimediatatenstrom in ein übertragbares Format zu bringen, wird schließlich noch der Anfangsblock vervollständigt (Schritt 112), derart, daß der Ausgabewert 46 in den bereits im Schritt 100 erstellten Anfangsblock eingetragen wird.

In Abweichung von dem in Fig. 4 dargestellten Ausführungsbeispiel kann die Schrittreihenfolge vertauscht werden. So könnte beispielsweise zunächst die gesamte Verschlüsselung des Multimediatatenschlüssels durchgeführt werden, woraufhin die Verschlüsselung der Multimediataten durchgeführt wird. Ferner könnte die Hash-Summe über den Anfangsblock ermittelt werden, bevor der Multimediatatenschlüssel generiert wird. Weitere Variationen sind möglich. Selbstverständlich kann der Schritt 108 erst dann durchgeführt werden, wenn die Hash-Summe ermittelt worden ist. Darüberhinaus kann der Schritt 110 erst dann durchgeführt werden, wenn der Basiswert vorliegt.

Vorzugsweise wird zum Verschlüsseln der Multimedia-Daten mit

dem Multimediataten-Schlüssel im Schritt 104 ein symmetrisches Verschlüsselungsverfahren eingesetzt, da hier unter Umständen relativ große Mengen an Daten ver- bzw. entschlüsselt werden müssen. Symmetrische Verschlüsselungsverfahren arbeiten, wie es bekannt ist, schneller als asymmetrische Verschlüsselungsverfahren, wie sie im Schritt 110 zum Verschlüsseln des Multimediatatenschlüssels eingesetzt werden.

Ferner wird es bevorzugt, daß der Multimediataten-Schlüssel K mittels eines Zufallszahlengenerators erzeugt wird, derart, daß der Basiswert, der in dem Schritt 108 erzeugt wird, für denselben Kunden jedesmal eine andere Form annimmt, um es einem Angreifer auf das cryptographische System so schwer als möglich zu machen.

Die Verknüpfungsoperation, um die Hash-Summe mit dem Multimediataten-Schlüssel K zu verknüpfen, sollte, wie es Bezugnehmend auf Fig. 5 noch erläutert wird, eine selbstinverse Verknüpfung sein. Eine solche selbstinverse Verknüpfung wäre die XOR- (Exklusiv-Oder-) Verknüpfung. Selbstinvers bedeutet, daß ein zweimaliges Anwenden dieser Verknüpfung zu einem Ergebnis führt, das gleich dem Ausgangswert ist. Außerdem ist es möglich, daß die Verknüpfungs-Funktion aus Fig. 5 die inverse Funktion derjenigen aus Fig. 4 ist. Die Verknüpfungsfunktion muß daher lediglich umkehrbar sein, d. h. zu derselben muß eine Umkehrfunktion existieren.

Im Schritt 110 wird gemäß der vorliegenden Erfindung ein asymmetrisches Verschlüsselungsverfahren ausgeführt. Wie es bekannt ist, existieren bei einem asymmetrischen Verschlüsselungsverfahren zwei Schlüssel, mit denen eine Ver- bzw. Entschlüsselung möglich ist, die jedoch voneinander unterschiedlich sind. Ein Schlüssel wird als privater Schlüssel P (Privat Key) bezeichnet, während der andere Schlüssel als der öffentliche Schlüssel Ö (Public Key) bezeichnet wird. Allgemein gesagt haben asymmetrische Verschlüsselungsverfahren die Eigenschaft, daß zu verschlüsselnde Daten, die mittels des privaten Schlüssels verschlüsselt worden sind,

mit dem öffentlichen Schlüssel wieder entschlüsselt werden können. Analog dazu können zu verschlüsselnde Daten, die mit dem öffentlichen Schlüssel verschlüsselt worden sind, wieder mit dem privaten Schlüssel entschlüsselt werden. Daraus ist zu sehen, daß die privaten und öffentlichen Schlüssel prinzipiell gegeneinander austauschbar sind.

Ein Aspekt der vorliegenden Erfindung besteht darin, daß der Anfangsblock über die Schritte 106 und 108 in die Verschlüsselung des Multimediatatenschlüssels miteinbezogen wird. Alternativ könnten jedoch auch Teile des Nutzdatenblocks miteinbezogen werden, wodurch aufgrund unerlaubter Manipulationen der Nutzdaten der gesamte Multimediatatenstrom unbrauchbar werden würde, da es dann nicht mehr möglich ist, den Multimediatatenschlüssel in der Entschlüsselungsvorrichtung zu berechnen.

Obwohl im Schritt 106 davon gesprochen wird, daß eine Hash-Summe über den Anfangsblock gebildet wird, sei darauf hingewiesen, daß jede Verarbeitung eines Teils des Multimediatatenstroms, um Informationen abzuleiten, die den Teil des Multimediatatenstrom kennzeichnen, eingesetzt werden könnte. Je aufwendiger der Hash-Algorithmus ist, der hier verwendet wird, umso sicherer wird der verschlüsselte Multimediatatenstrom gegenüber Angreifern, die ihn knacken wollen, um beispielsweise die Lizenzinformationen bzw. die Distributor- oder Benutzer-Informationen in ihrem (unerlaubten) Sinne zu modifizierten.

Im nachfolgenden wird auf Fig. 5 Bezug genommen, die ein Flußdiagramm des Entschlüsselungsverfahrens zeigt, das möglicherweise von einem Kunden durchgeführt wird. In einem Schritt 120 liest der Kunde zunächst den Ausgabewert aus dem Anfangsblock des verschlüsselten Multimediatatenstroms. Er führt daraufhin eine Entschlüsselung dieses Ausgabewerts mittels der entsprechenden asymmetrischen Entschlüsselung durch (Schritt 122). Hierauf bildet die Entschlüsselungsvorrichtung beim Kunden wieder eine Hash-Summe über den An-

fangsblock, wobei die bestimmten Teile, die beim Verschlüsseln einen vordefinierten Wert hatten, in einem Schritt 124 ebenfalls den gleichen vordefinierten Wert erhalten. Anschließend wird die Hash-Summe mit dem entschlüsselten Ausgabewert (Schritt 122) verknüpft, woraus sich der Multimediatatenschlüssel ergibt (Schritt 126). In einem Schritt 128 werden schließlich die verschlüsselten Multimediataten mit dem in dem Schritt 126 erhaltenen Multimediatatenschlüssel entschlüsselt.

Es zeigt sich, daß das Entschlüsselungsverfahren im wesentlichen die Umkehrung des Verschlüsselungsverfahrens, das anhand des Flußdiagramms von Fig. 4 beschrieben worden ist, darstellt. Selbstverständlich können auch bei dem in Fig. 5 gezeigten Entschlüsselungsverfahren mehrere Schritte vertauscht werden. So könnte beispielsweise zunächst die Hash-Summe über den Anfangsblock gebildet werden (Schritt 124), wonach der Ausgabewert mit dem öffentlichen Schlüssel entschlüsselt wird (Schritt 122). Auch das Lesen des Ausgabewerts aus dem Anfangsblock (Schritt 120) können beispielsweise erst nach dem Schritt 124, jedoch unbedingt vor dem Schritt 126 durchgeführt werden. Auch Schritt 128 ist erst möglich, nachdem der Schritt 126 durchgeführt worden ist, da der den Multimediatatenschlüssel ergibt.

Das in Fig. 5 gezeigte Entschlüsselungsverfahren bringt anhand des Schritts 124 noch einmal deutlich zum Ausdruck, was passiert, wenn ein Kunden den Anfangsblock 12 modifiziert hat, der ja üblicherweise unverschlüsselt ist und ohne weiteres für Angriffe zugänglich ist. Eine Änderung der Lizenzinformationen, beispielsweise des Anfangs- und des Enddatums würde jedoch unweigerlich dazu führen, daß die Hash-Summe über den Anfangsblock, die im Schritt 124 gebildet wird, einen anderen Wert hat wie die Hash-Summe die im Schritt 106 (Fig. 4) während der Verschlüsselung gebildet worden ist. Die erneute Verknüpfung der Hash-Summe im Schritt 126 (Fig. 5) wird daher nicht mehr zu dem korrekten Multimediatatenschlüssel führen, da die beiden Hash-Summen, d. h. die

Hash-Summe während des Verschlüsseln und die Hash-Summe während des Entschlüsseln, voneinander unterschiedlich sind. Somit sind die gesamten Multimediadaten unbrauchbar, da sie nicht mehr korrekt entschlüsselt werden können, da es nicht mehr möglich ist, aufgrund der Manipulation am Anfangsblock den Multimediadatenschlüssel zu berechnen, den die Verschlüsselungsvorrichtung eingesetzt hat. Jede Änderung am Anfangsblock führt somit automatisch zur Zerstörung der Multimediadaten selbst.

Patentansprüche

1. Verfahren zum Erzeugen eines Nutzdatenstroms (10), der einen Anfangsblock (12) und einen Nutzdatenblock (14) mit verschlüsselten Nutzdaten aufweist, mit folgenden Schritten:

Generieren (102) eines Nutzdaten-Schlüssels für einen Nutzdaten-Verschlüsselungsalgorithmus zum Verschlüsseln von Nutzdaten;

Verschlüsseln (104) von Nutzdaten unter Verwendung des Nutzdaten-Schlüssels und des Nutzdaten-Verschlüsselungsalgorithmus, um einen verschlüsselten Abschnitt (16) des Nutzdatenblocks (14) des Nutzdatenstroms (10) zu erhalten;

Verarbeiten (106) eines Teils des Nutzdatenstroms (10), um Informationen abzuleiten, die den Teil des Nutzdatenstroms kennzeichnen;

Verknüpfen (108) der Informationen mit dem Nutzdatenschlüssel mittels einer invertierbaren logischen Verknüpfung, um einen Basiswert zu erhalten;

Verschlüsseln (110) des Basiswerts unter Verwendung eines Schlüssels von zwei zueinander unterschiedlichen Schlüsseln (P, Ö) mit einem asymmetrischen Verschlüsselungsverfahren, wobei die zwei unterschiedlichen Schlüssel der öffentliche (Ö) bzw. der private (P) Schlüssel für das asymmetrische Verschlüsselungsverfahren sind, um einen Ausgabewert (46) zu erhalten, der eine verschlüsselte Version des Nutzdatenschlüssels ist; und

Eintragen (112) des Ausgabewerts (46) in den Anfangsblock (12) des Nutzdatenstroms (10).

2. Verfahren nach Anspruch 1, bei dem der Nutzdaten-Verschlüsselungsalgorithmus ein symmetrischer Verschlüsselungsalgorithmus ist.
3. Verfahren nach Anspruch 1 oder 2, bei dem die invertierbare logische Verknüpfung selbst-invertierend ist und eine EXKLUSIV-ODER-Verknüpfung umfaßt.
4. Verfahren nach einem der vorhergehenden Ansprüche, bei dem der eine Schlüssel der zwei voneinander unterschiedlichen Schlüssel (P, Ö) der private Schlüssel (P) eines Erzeugers des Nutzdatenstroms ist oder der öffentliche Schlüssel (Ö) eines Konsumenten des Nutzdatenstroms ist.
5. Verfahren nach einem der vorhergehenden Ansprüche, bei dem der Teil des Nutz-Datenstroms, der verarbeitet wird (106), um die Informationen abzuleiten, zumindest einen Teil des Anfangsblocks (12) umfaßt.
6. Verfahren nach einem der vorhergehenden Ansprüche, bei dem der Schritt des Verarbeitens (106) das Bilden einer Hash-Summe aufweist.
7. Verfahren nach einem der vorhergehenden Ansprüche, das ferner folgenden Schritt aufweist:

Identifizieren des Algorithmus, der im Schritt des Verarbeitens (106) verwendet wird, durch einen Eintrag (68) in den Anfangsblock.

8. Verfahren nach einem der vorhergehenden Ansprüche, das ferner folgenden Schritt aufweist:

Eintragen von Lizenzdaten (30) in den Anfangsblock (12), die sich darauf beziehen, in welcher Weise der Nutzdatenstrom (10) verwendet werden darf.

9. Verfahren nach Anspruch 8, bei dem die Lizenzdaten (30) angeben, wie oft der Nutzdatenstrom abgespielt werden darf (58) und wie oft er bereits abgespielt wurde (60).
10. Verfahren nach Anspruch 8 oder 9, bei dem die Lizenzdaten (30) angeben, wie oft der Inhalt des Nutzdatenstroms kopiert werden darf (62), und wie oft er bereits kopiert worden ist (64).
11. Verfahren nach einem der Ansprüche 8 bis 10, bei dem die Lizenzdaten (30) angeben, ab wann der Nutzdatenstrom nicht mehr benutzt werden darf (54).
12. Verfahren nach einem der Ansprüche 8 bis 11, bei dem die Lizenzdaten (30) angeben, ab wann der Nutzdatenstrom entschlüsselt werden darf (56).
13. Verfahren nach einem der Ansprüche 8 bis 12, bei dem der Teil des Nutzdatenstroms, der verarbeitet wird, um die Informationen abzuleiten (106) die Lizenzdaten (30) umfaßt.
14. Verfahren nach einem der vorhergehenden Ansprüche, bei dem der Schritt des Verarbeitens ferner folgende Teilschritte aufweist:

Setzen des Eintrags (46) für den Ausgabewert in dem Anfangsblock (12) auf einen definierten Wert, und Verarbeiten (106) des gesamten Anfangsblocks einschließlich des auf einen definierten Wert gesetzten Eintrags (46).
15. Verfahren nach einem der vorhergehenden Ansprüche, das ferner folgende Schritte aufweist:

Identifizieren des Lieferanten (42) des Nutzdatenstroms durch einen Lieferanteneintrag (42) in den Anfangsblock (12);

Identifizieren des Benutzers (44) des Nutzdatenstroms durch einen Benutzereintrag (44) in den Anfangsblock (12) des Nutzdatenstroms,

wobei der Lieferanteneintrag (42) und der Benutzereintrag (44) zu dem Teil des Nutzdatenstroms (10) gehören, der verarbeitet wird (106), um die Informationen abzuleiten.

16. Verfahren nach einem der vorhergehenden Ansprüche, das ferner folgenden Schritt aufweist:

Identifizieren des Nutzdaten-Verschlüsselungsalgorithmus durch einen Eintrag (40) in den Anfangsblock (12) des Nutzdatenstroms (10).

17. Verfahren zum Entschlüsseln eines verschlüsselten Nutzdatenstroms (10), der einen Anfangsblock (12) und einen Nutzdatenblock (14) mit verschlüsselten Nutzdaten aufweist, wobei der Anfangsblock (12) einen Ausgabewert (46) aufweist, der durch eine Verschlüsselung eines Basiswerts mit einem asymmetrischen Verschlüsselungsverfahren unter Verwendung eines Schlüssels von zwei unterschiedlichen Schlüsseln (P, Ö), die einen privaten (P) und einen öffentlichen (Ö) Schlüssel umfassen, erzeugt worden ist, wobei der Basiswert eine Verknüpfung eines Nutzdatenschlüssels, mit dem die verschlüsselten Nutzdaten unter Verwendung eines Nutzdaten-Verschlüsselungsalgorithmus verschlüsselt sind, mit durch eine bestimmte Verarbeitung abgeleiteten Informationen, die einen bestimmten Teil des Nutzdatenstroms (10) eindeutig kennzeichnen, darstellt, mit folgenden Schritten:

Erhalten (120) des Ausgabewerts (46) aus dem Anfangsblock (12);

Entschlüsseln (122) des Ausgabewerts (46) unter Verwendung des anderen Schlüssels des asymmetrischen Ver-

schlüsselungsverfahrens, um den Basiswert zu erhalten;

Verarbeiten (124) eines Teils des Nutzdatenstroms (10) unter Verwendung des beim Verschlüsseln verwendeten Verarbeitungsverfahrens, um Informationen abzuleiten, die den Teil kennzeichnen, wobei der Teil dem bestimmten Teil beim Verschlüsseln entspricht;

Verknüpfen (126) der Informationen mit dem Basiswert unter Verwendung der entsprechenden Verknüpfung, wie sie beim Verschlüsseln verwendet wurde, um den Nutzdatenschlüssel zu erhalten; und

Entschlüsseln (128) des Blocks (14) mit verschlüsselten Nutzdaten unter Verwendung des Nutzdaten-Schlüssels und des beim Verschlüsseln verwendeten Nutzdaten-Verschlüsselungsalgorithmus.

18. Verfahren nach Anspruch 17, bei dem der Anfangsblock (12) Lizenzinformationen (30) aufweist, die sich darauf beziehen, in welcher Weise der Nutzdatenstrom (10) verwendet werden kann.
19. Verfahren nach Anspruch 17 oder 18, bei dem der Teil, der verarbeitet wird, um die Informationen abzuleiten, der Anfangsblock (12) ist.
20. Verfahren nach Anspruch 18 oder 19, das ferner folgenden Schritt aufweist:

Überprüfen, ob die Lizenzinformationen (30) ein Entschlüsseln erlauben; und

falls ein Entschlüsseln nicht erlaubt ist, Abbrechen des Entschlüsselungsverfahrens.
21. Verfahren nach einem der Ansprüche 17 bis 20, bei dem der Anfangsblock (12) einen Benutzereintrag (44) auf-

weist, das ferner folgende Schritte aufweist:

Überprüfen, ob ein aktueller Benutzer autorisiert ist, anhand des Benutzereintrags (44); und

falls der Benutzer nicht autorisiert ist, Abbrechen des Entschlüsselungsverfahrens.

22. Verfahren nach einem der Ansprüche 17 bis 21, bei dem der eine Schlüssel, der beim Verschlüsseln verwendet wurde, der private Schlüssel (P) des asymmetrischen Verschlüsselungsverfahrens ist, während der andere Schlüssel, der beim Entschlüsseln verwendet wird, der öffentliche Schlüssel (Ö) des asymmetrischen Verschlüsselungsverfahrens ist.
23. Verfahren nach einem der Ansprüche 17 bis 21, bei dem der eine Schlüssel, der beim Verschlüsseln verwendet wurde, der öffentliche Schlüssel (Ö) des asymmetrischen Verschlüsselungsverfahrens ist, während der andere Schlüssel, der beim Entschlüsseln verwendet wird, der private Schlüssel (P) des asymmetrischen Verschlüsselungsverfahrens ist.
24. Verfahren nach einem der Ansprüche 17 bis 23, bei dem der Schritt des Verarbeitens (124) das Bilden einer Hash-Summe umfaßt.
25. Verfahren nach einem der Ansprüche 17 bis 24, bei dem ein Teil des Anfangsblocks (12), der beim Verschlüsseln für den Schritt des Verarbeitens auf einen definierten Wert gesetzt wurde, beim Entschlüsseln für den Schritt des Verarbeitens (124) auf denselben definierten Wert gesetzt wird.
26. Verfahren nach Anspruch 25, bei dem der Teil des Anfangsblocks (12), der auf einen definierten Wert gesetzt wird, den Eintrag für den Ausgabewert (46) des

Anfangsblocks (12) umfaßt.

27. Verfahren nach einem der Ansprüche 17 bis 26, bei dem der Schritt des Verknüpfens (126) das Verwenden einer EXKLUSIV-ODER-Verknüpfung aufweist.

28. Vorrichtung zum Erzeugen eines verschlüsselten Nutzdatenstroms, der einen Anfangsblock (12) und einen Nutzdatenblock (14) mit verschlüsselten Nutzdaten aufweist, mit folgenden Merkmalen:

einer Einrichtung zum Generieren (102) eines Nutzdaten-Schlüssels für einen Nutzdaten-Verschlüsselungsalgorithmus zum Verschlüsseln von Nutzdaten;

einer Einrichtung zum Verschlüsseln (104) von Nutzdaten unter Verwendung des Nutzdaten-Schlüssels und des Nutzdaten-Verschlüsselungsalgorithmus, um einen verschlüsselten Abschnitt (16) des Nutzdatenblocks (14) des Nutzdatenstroms (10) zu erhalten;

einer Einrichtung zum Verarbeiten (106) eines Teils des Nutzdatenstroms (10), um Informationen abzuleiten, die den Teil des Nutzdatenstroms kennzeichnen;

einer Einrichtung zum Verknüpfen (108) der Informationen mit dem Nutzdatenschlüssels mittels einer invertierbaren logischen Verknüpfung, um einen Basiswert zu erhalten;

einer Einrichtung zum Verschlüsseln (110) des Basiswerts unter Verwendung eines Schlüssels von zwei zueinander unterschiedlichen Schlüsseln (P, Ö) mit einem asymmetrischen Verschlüsselungsverfahren, wobei die zwei unterschiedlichen Schlüssel der öffentliche (Ö) bzw. der private (P) Schlüssel für das asymmetrische Verschlüsselungsverfahren sind, um einen Ausgabewert (46) zu erhalten, der eine verschlüsselte Version des

Nutzdatenschlüssels ist; und

einer Einrichtung zum Eintragen (112) des Ausgabewerts (46) in den Anfangsblock (12) des Nutzdatenstroms (10).

29. Vorrichtung zum Entschlüsseln eines verschlüsselten Nutzdatenstroms (10), der einen Anfangsblock (12) und einen Block (14) mit verschlüsselten Nutzdaten aufweist, wobei der Anfangsblock (12) einen Ausgabewert (46) aufweist, der durch eine Verschlüsselung eines Basiswerts mit einem asymmetrischen Verschlüsselungsverfahren unter Verwendung eines Schlüssels von zwei unterschiedlichen Schlüsseln (P, Ö), die einen privaten (P) und einen öffentlichen (Ö) Schlüssel umfassen, erzeugt worden ist, wobei der Basiswert eine Verknüpfung eines Nutzdatenschlüssels, mit dem die verschlüsselten Nutzdaten unter Verwendung eines Nutzdaten-Verschlüsselungsalgorithmus verschlüsselt sind, von durch eine bestimmte Verarbeitung abgeleiteten Informationen, die einen bestimmten Teil des Nutzdatenstroms (10) eindeutig kennzeichnen, darstellt, mit folgenden Merkmalen:

einer Einrichtung zum Erhalten (120) des Ausgabewerts (46) aus dem Anfangsblock (12);

einer Einrichtung zum Entschlüsseln (122) des Ausgabewerts (46) unter Verwendung des anderen Schlüssels (Ö) und des asymmetrischen Verschlüsselungsverfahrens, um den Basiswert zu erhalten;

einer Einrichtung zum Verarbeiten (124) eines Teils des Nutzdatenstroms (10) unter Verwendung des beim Verschlüsseln verwendeten Verarbeitungsverfahrens, um Informationen abzuleiten, die den Teil kennzeichnen, wobei der Teil dem bestimmten Teil beim Verschlüsseln entspricht;

einer Einrichtung zum Verknüpfen (126) der Informatio-

nen mit dem Basiswert unter Verwendung der entsprechenden Verknüpfung, wie sie beim Verschlüsseln verwendet wurde, um den Nutzdatenschlüssel zu erhalten; und

einer Einrichtung zum Entschlüsseln (128) des Blocks (14) mit verschlüsselten Nutzdaten unter Verwendung des Nutzdaten-Schlüssels und des beim Verschlüsseln verwendeten Nutzdaten-Verschlüsselungsalgorithmus.

30. Vorrichtung nach Anspruch 28 oder 29, die als Personalcomputer, als Stereoanlage, als Auto-HiFi-Gerät, als Solid-State-Player oder als Abspielgerät mit Festplatte oder CD-ROM ausgeführt ist.

**Verfahren und Vorrichtung zum Erzeugen eines verschlüsselten
Nutzdatenstroms und Verfahren und Vorrichtung zum
Entschlüsseln eines verschlüsselten Nutzdatenstroms**

Zusammenfassung

Bei einem Verfahren zum Erzeugen eines verschlüsselten Nutzdatenstroms, der einen Anfangsblock und einen Block mit verschlüsselten Nutzdaten aufweist, wird ein Nutzdatenschlüssel für einen Nutzdaten-Verschlüsselungsalgorithmus zum Verschlüsseln von Nutzdaten generiert (102). Die Nutzdaten werden unter Verwendung des generierten Nutzdatenschlüssels und des Nutzdaten-Verschlüsselungsalgorithmus verschlüsselt (104), um den Block mit verschlüsselten Nutzdaten des Nutzdatenstroms zu erhalten. Ein Teil des Nutzdatenstroms wird verarbeitet (106), um Informationen abzuleiten, die den Teil des Nutzdatenstroms kennzeichnen. Die Informationen werden mit den Nutzdaten mittels eines invertierbaren logischen Verknüpfung verknüpft (108), um einen Basiswert zu erhalten. Dieser Basiswert wird schließlich unter Verwendung eines Schlüssels von zwei zueinander unterschiedlichen Schlüsseln mit einem asymmetrischen Verschlüsselungsverfahren verschlüsselt (110), wobei die zwei unterschiedlichen Schlüssel der öffentliche bzw. der private Schlüssel für das asymmetrische Verschlüsselungsverfahren sind, um einen Ausgabewert zu erhalten, der eine verschlüsselte Version des Nutzdatenschlüssels ist. Der Ausgabewert wird schließlich in den Anfangsblock eingetragen, um den Nutzdatenstrom fertigzustellen (112). Änderungen an dem Anfangsblock bzw. an den Nutzdaten selbst, die nicht autorisiert sind, führen zu einer automatischen Zerstörung der Nutzdaten.

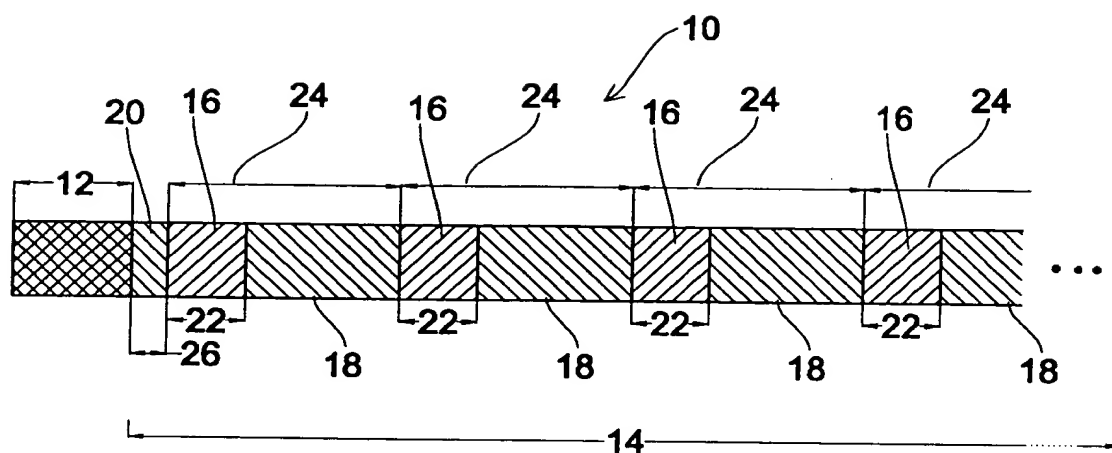


Fig. 1

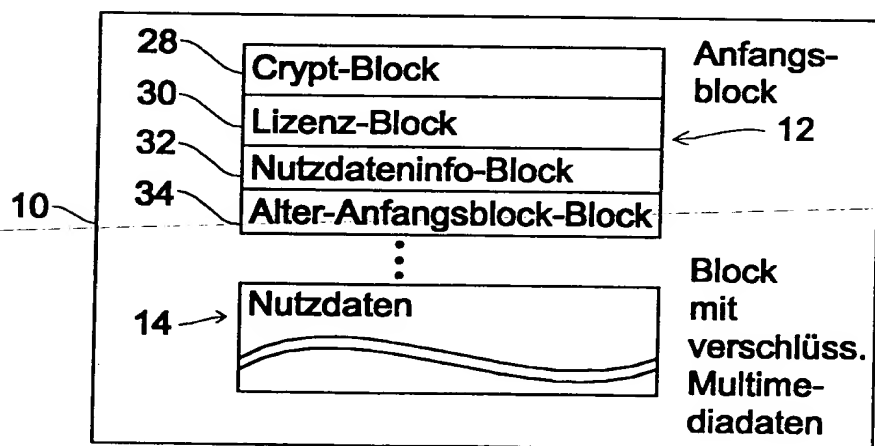


Fig. 2

107

28	Crypt-Block	MMD-Verschlüss.-algorithmus		40
		Erster Schritt		26
		Schritt		24
		Menge		22
		Distributor		42
		Benutzer		44
		Ausgabewertlänge		48
		Ausgabewertmaske		50
		Ausgabewert	X	46
				52
30	Lizenz-Block	Bitmaske		54
		Verfallsdatum		56
		Anfangsdatum		58
		Erlaubte Abspielanzahl		60
		Tatsächliche Abspielanzahl	X	62
		Erlaubte Kopieanzahl		64
32	Nutzdaten-Info-Block	Tatsächliche Kopieanzahl	X	66
		Hashsumme über Anf.Block	X	68
34	Alter-Anfangsblock-Block	Typ des Hashalgorithmus		70
		Alter Anfangsblock	X	
14	Nutzdaten-Block			
		Nutzdaten-Typ		
		NUTZDATEN		

Fig. 3

BEIM DISTRIBUTOR

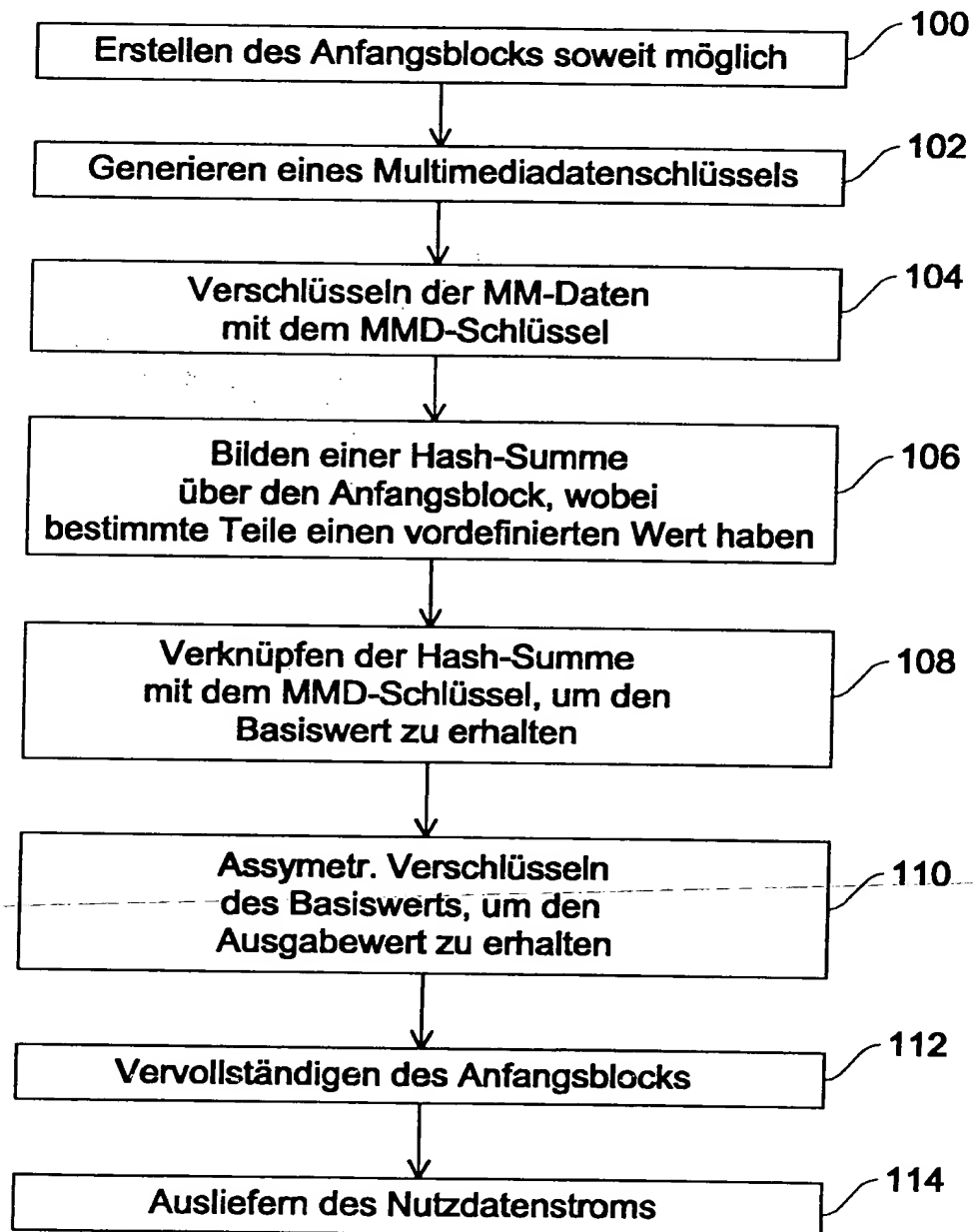


Fig. 4

BEIM KUNDEN

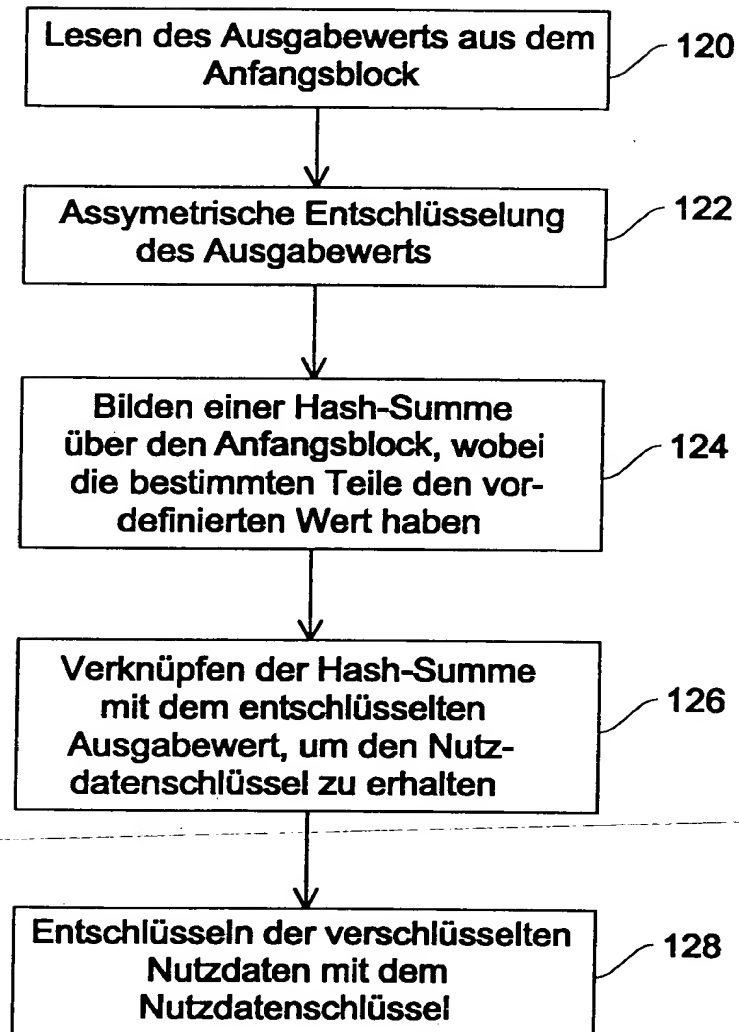


Fig. 5

PATENT COOPERATION TREATY

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

Commissioner
 US Department of Commerce
 United States Patent and Trademark
 Office, PCT
 2011 South Clark Place Room
 CP2/5C24
 Arlington, VA 22202
 ETATS-UNIS D'AMERIQUE
 in its capacity as elected Office

Date of mailing (day/month/year) 01 November 2000 (01.11.00)	
International application No. PCT/EP99/09981	Applicant's or agent's file reference FH991202.PCT
International filing date (day/month/year) 15 December 1999 (15.12.99)	Priority date (day/month/year) 16 February 1999 (16.02.99)
Applicant RUMP, Niels et al	

1. The designated Office is hereby notified of its election made:



in the demand filed with the International Preliminary Examining Authority on:

13 September 2000 (13.09.00)



in a notice effecting later election filed with the International Bureau on:

2. The election ☒ was

was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No.: (41-22) 740.14.35	Authorized officer Zakaria EL KHODARY Telephone No.: (41-22) 338.83.38
---	--

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.